TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2,00 €

HACKER JOURNAL

n. 163
www.hackerjournal.it



PHORM lo spione
ECCO COME FUNZIONA

CRYPTO
CIFRATURA INVIOLABILE: LA MIA!

GAMES
CIAK! Hacker si gira

SOFTWARE
OpenOffice 3.0

FACEBOOK
PORTE APERTE ALL'HACKER

QUATTORD. ANNO 8 - N° 163 - 6/19 NOVEMBRE 2008 - €2,00
WLF PUBLISHING

hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



L'hacking è uguale per tutti

"La vera libertà di stampa è dire alla gente ciò che la gente non vorrebbe sentirsi dire."
George Orwell

È di pochi giorni fa la notizia che il conto bancario di Nicolas Sarkozy, primo ministro francese, è stato violato. "Truffatori telematici sono riusciti a procurarsi le coordinate bancarie del conto personale del presidente francese Nicolas Sarkozy e hanno effettuato vari prelievi". Lo scrive il quotidiano francese Journal du Dimanche.

La notizia si è diffusa il 19 ottobre ma il fatto sarebbe avvenuto a settembre. I truffatori hanno intelligentemente prelevato piccole somme così da non far insospettire il proprietario del conto. La truffa, pur essendo effettuata con l'accesso on-line al conto, non è stata operata con una tecnica di attacco verso il sito della banca ma probabilmente i truffatori si sono impossessati dei codici di accesso in maniera diretta.

Se fai un minimo di ricerca on-line sulla notizia ti accorgerai come si passi velocemente da "Frode on line per Sarkozy" (Corriere.it) a "Clonata la carta di credito di Sarkozy" (Repubblica.it) fino al più allarmistico "Francia: gli hacker attaccano il conto in banca del..." (Informazione.it). Se hai qualche minuto da perdere puoi inoltre divertirti a leggere come le diverse redazioni propongono la (stessa) notizia...

Questa, per quanto di per sé piuttosto banale, lascia spazio ad alcune riflessioni:

- *Neanche il conto del primo ministro è sicuro, figuriamoci il nostro.*
- *Controllate sempre i vostri estratti conto, anche per le piccole spese.*
- *Il primo ministro francese, pur essendo un politico, non ha sollevato un superpolverone accusando hacker, i suoi oppositori, la comunità Internet nel suo insieme o imprecisate lobbie.*
- *Né il presidente, né altri politici francesi, per una volta tanto, hanno invocato misure straordinarie contro la Rete e i suoi frequentatori, proponendo magari leggi che obbligassero chiunque abbia un conto on-line di certificare direttamente in banca ogni operazione. In Italia sarebbe stata la stessa cosa?*
- *Come purtroppo avviene nella maggior parte dei casi la notizia è stata riportata in maniera differente e modificandone i particolari.*

Ormai siamo fin troppo abituati alla disinformazione su tutto ciò che riguarda il Web, siamo abituati all'abuso della parola hacker, siamo abituati a politici che di Internet sanno poco o nulla.

L'unico sistema per sviluppare un senso critico rimane l'approfondimento e la ricerca di informazioni da più fonti. Mi raccomando: stai sempre all'erta.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 8 – N.163
6/19 novembre 2008

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

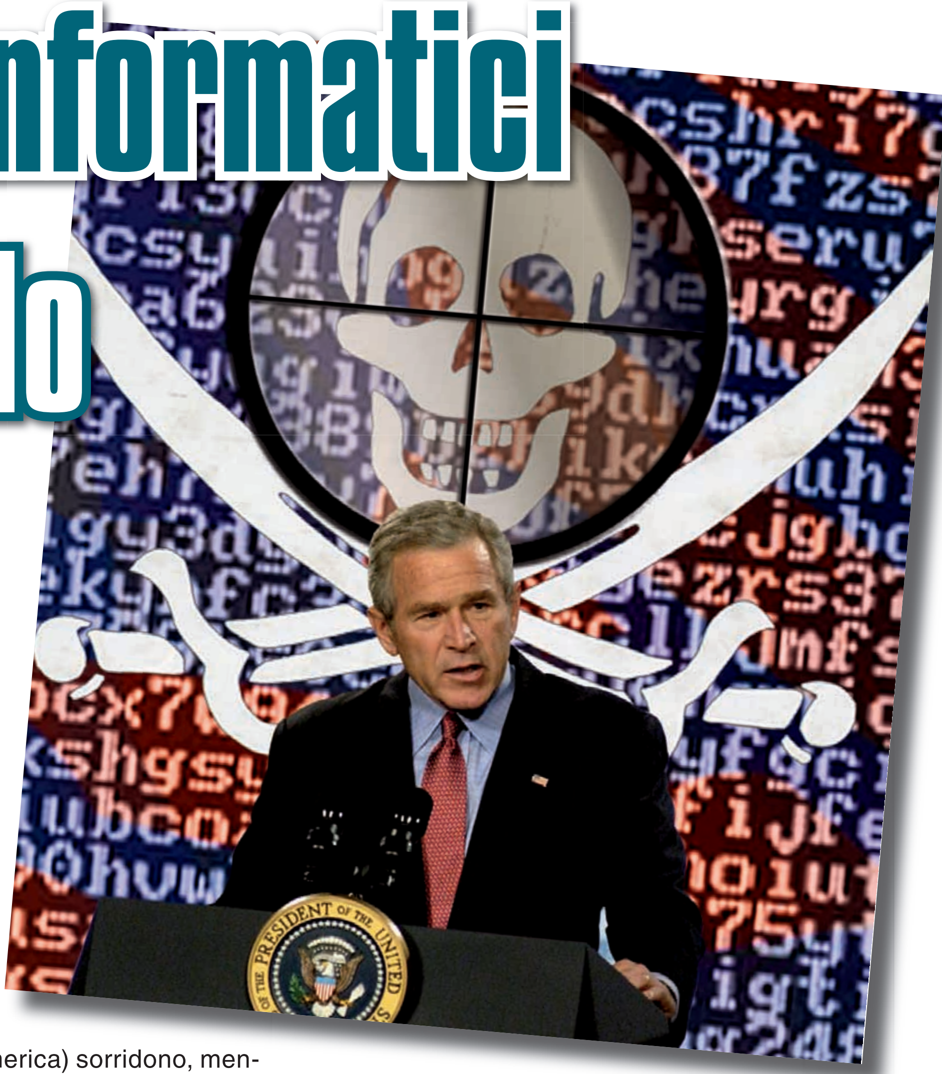
Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Bush contro i pirati informatici E non solo



Il presidente americano Bush ha firmato una nuova legge che stabilisce pesanti sanzioni a livello federale per i crimini di pirateria e contraffazione lesivi delle norme sulla tutela dei diritti d'autore. Non è una novità, e come al solito si formano due blocchi distinti, a favore e contrari alla nuova legge, ma stavolta a sollevare critiche non è il popolo del peer to peer ma addirittura il Dipartimento di Giustizia degli Stati Uniti.

Secondo il Dipartimento questa legge va a ledere la sua autorità, dando ad altri la possibilità di vigilare sull'uso degli strumenti informatici da parte degli utenti per verificare che non si usino per operazioni di duplicazione e distribuzione illecita di materiale protetto da diritto d'autore.

Le nuove norme indicano che gli Stati Uniti potranno intervenire sul proprio territorio e internazionalmente per proteggere "l'innovazione americana". Come dire, attenti se scaricate CD di artisti americani, potreste trovarvi l'FBI che vi aspetta a colazione. Contenti, RIAA (Recording Industry Association of America) e MPAA (Motion Picture Association of America) sorridono, mentre critici e associazioni per la protezione dei diritti civili insorgono perché questa legge rischia di far punire persone che invece non hanno commesso reati. Inoltre sostengono che i reati di pirateria e contraffazione stanno diminuendo e sono contrari a norme che applichino forfait sulle attrezzature informatiche che possono essere usate per compiere tali reati (come la tassa sui supporti vergini qui in Italia): pensiamo ad esempio a un computer che viene usato da una persona per studiare e da un'altra per scaricare musica e film. Inoltre, l'industria può già avviare cause contro reati di pirateria e molti procedimenti sono già in corso, rendendo superflua questa nuova legge.

Ci preoccupa la possibilità dell'intervento americano in campo internazionale. Senza voler diventare antimoralisti, che gli altri vengano a farci le leggi a casa nostra proprio non ci va giù...

BYE BYE MOUSE!

Ci stanno studiando su diverse aziende, prima fra tutte Microsoft, e pare che ciò che trapela dalle strette maglie della segretezza aziendale sia sufficiente per accendere gli animi del popolo dei computerofili internettiani. Niente più mouse, tastiere e monitor, faremo tutto direttamente pasticciando con le mani su un tavolo che funge da display, da periferica di input e da periferica di puntamento, con una danza di movimenti di mani e dita che magicamente farà muovere una finestra o ruotare una fotografia. Oahu, questo il nome in codice della tecnologia in fase di test da parte di Microsoft, che sta valutando anche quali potrebbero essere le reazioni del pubblico qualora diventasse un prodotto in commercio.



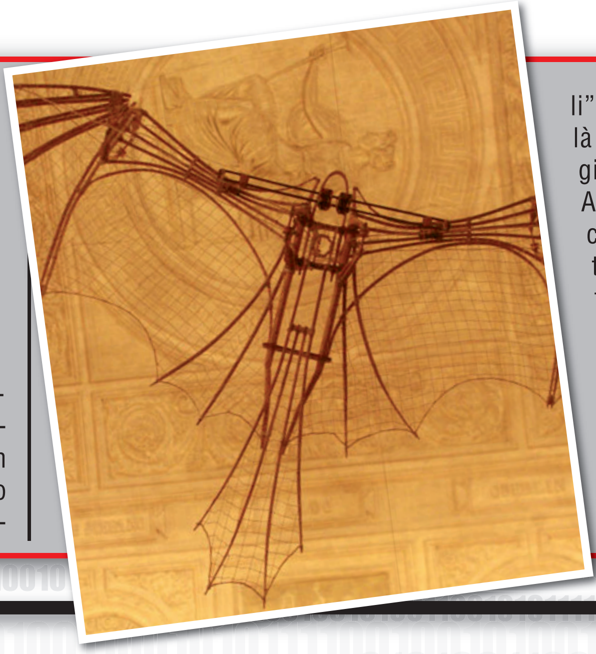
SKYPE SPIATO IN CINA

Gli utenti cinesi di Skype sono avvisati: meglio tornare ai tam-tam e ai segnali di fumo. Pare infatti che TOM Online, il provider che ha portato Skype in Cina, non solo offra il servizio, ma anche lo controlli in toto, registrando in enormi archivi addirittura intere conversazioni tra utenti. L'ha scoperto un ricercatore canadese in Cina per lavoro: ogni volta che scriveva una parolaccia sul suo Skype, notava una strana richiesta TCP verso un server di TOM Online dove, riuscendo a entrare dopo aver smanettato un po' con Python, trovava un archivio distribuito su ben otto server contenente dati anagrafici, numeri di carte di credito e di telefono e le conversazioni degli utenti Skype salvate in modo che possano essere tracciate geograficamente e cronologicamente. In pratica, alcune parole scritte via messenger o SMS funzionano da trigger che attiva l'oscuramento e inizia la registrazione dell'attività dell'utente che le ha scritte. Ma lo sappiamo bene ormai, la libertà di pensiero e la privacy in Cina sono solo belle parole.



BREVETTO RICORSIVO

Sono sinceramente preoccupato. Non sono un fanatico del "no patents" a tutti i costi, anche se sono contrario a chi tenta di brevettare la ruota o l'acqua calda a spese di milioni di utenti in tutto il mondo. È proprio quello che sta facendo IBM: ha richiesto infatti il riconoscimento di un brevetto per una tecnologia in grado di cercare spazi liberi e "colonizzabili" tra i brevetti altrui, per arrivare là dove nessun'altra azienda è mai giunta prima.



Assurdo, siamo arrivati al punto in cui chi detiene dei diritti/brevetti è tanto potente da potersi permettere di sprecare tempo e risorse non su progetti definiti, focalizzati e sostanzialmente utili, ma per cercare scappatoie e potenziali brevetti non assegnati per poterseli accaparrare prima degli altri. Vi lascio alle vostre conclusioni.

VERA MINACCIA O ENNESIMA OPERAZIONE COMMERCIALE?

Alcuni ricercatori hanno scoperto una nuova minaccia per la sicurezza su Internet: si tratta di una falla nella struttura dello stack TCP che permetterebbe a chiunque disponga di un PC e di una connessione DSL di bloccare qualunque server disponibile sulla Rete. Non usando una botnet: semplicemente usando il proprio PC e un software che, spendendo pochissimo in termini di risorse e di banda, è in grado di inondare un server di richieste che assorbono notevoli risorse sulla macchina causandone il blocco totale (cioè bisogna riavviarla a mano per rendere disponibile di nuovo il servizio). C'è chi però è scettico davanti ad annunci di questo tipo: Fyodor, l'autore di NMap, dice che "con tutto il rispetto per il loro lavoro, fare annunci di questo tipo senza però divulgarne i dettagli sa più di operazione di marketing che di segnale di allarme". Staremo a vedere.



PROFILI PROTETTI

I garanti della privacy di 70 Paesi del mondo si sono recentemente riuniti a Strasburgo. Tra le decisioni prese spicca il divieto di indicizzazione dei profili degli utenti dei siti di social networking da parte dei motori di ricerca, a meno che gli utenti stessi non lo permettano esplicitamente. Questa decisione arriva dopo che attraverso siti come MySpace si sono verificati fatti come la diffusione della notizia della gravidanza della figlia di Sarah Palin, candidata repubblicana alla vicepresidenza degli Stati Uniti o l'assassinio della ex moglie da parte di uno squilibrato dopo aver visto che su questi siti lei si era definita single.



ANDROID SOFT-KILLER

Si tratta di una condizione ben espressa nell'accordo di Android Market, il sistema con cui gli sviluppatori per la piattaforma possono mettere a disposizione degli utenti i propri programmi. Se trova su un terminale un software che violi tale accordo, Google può rimuoverlo arbitrariamente da remoto senza chiedere il consenso. Un po' come ha fatto Apple con gli iPhone, ma qui la differenza sta nel fatto che il controllo viene fatto a posteriori, non prima della diffusione del software. In pratica, Apple verifica il programma e in caso lo blocca, mentre Google lascia passare tutto ma se lo trova sul terminale è in grado di rimuoverlo. Ovvio che a questo punto tutti gli utenti Android si sentiranno controllati uno per uno, e non si sa bene ancora con quale diritto da parte di Google...

Facebook: c'è chi va, c'è chi viene

Si è tenuto lo scorso 11 ottobre il mega party degli utenti italiani di Facebook, che si sono ritrovati sotto il tendone dello Spazio Zero Village di Tor Quinto (Roma) per incontrarsi di persona. Circa 3000 gli intervenuti, alcuni entusiasti per l'evento, alcuni invece no perché non hanno incontrato gli amici virtuali. Intanto giunge la notizia che Dustin Moskovitz, co-fondatore di Facebook, e Justin Rosenstein, uno dei responsabili tecnici, lasceranno presto l'azienda malgrado l'enorme successo riscosso. Non è dato saperne il perché, ma pare che il fondatore e attuale CEO Mark Zuckerberg si stia ritrovando sempre più solo in un'impresa che ha proprio lo scopo opposto...



IN ARRIVO WINDOWS 7

Probabilmente Windows Vista non lascerà un buon ricordo dietro di sé nel momento in cui uscirà di scena, andando a fare buona (o cattiva, secondo il punto di vista) compagnia a obrobri come Windows ME. Intanto Microsoft si prepara al rilascio del suo successore, di cui si è parlato a Los Angeles nell'ambito della recente Professional Developers Conference. Al momento è stato anche svelato quale sarà il suo nome ufficiale: Windows 7 rimarrà per l'appunto Windows 7, senza alcun nome di fantasia come XP o Vista e senza riferimenti all'anno come in 98 o 2000. Oltre a essere la prima volta che il nome in codice di un sistema operativo rimane ufficiale al momento del rilascio, Microsoft vuole rimarcare il fatto che si tratta di un successore di vista e non un suo derivato, da qui il nome che ritorna un po' alle origini (come in Windows 3). Ma se la politica dei prezzi di Microsoft non cambia, probabilmente avremo davanti un altro compagno degno di ME e Vista...

SMARTPHONE A RISCHIO

Secondo alcuni esperti del Georgia Institute of Technology, la continua evoluzione degli smartphone (come l'iPhone) e del relativo software potrebbe ben preso entrare nelle mire degli hacker e dei cracker di tutto il mondo. Questi dispositivi stanno aumentando di numero in maniera esponenziale, usano software che permette l'accesso facile alla Rete e sono sempre più complessi, quindi sempre più a rischio di bug e di falle di sicurezza.

Sempre secondo questi esperti, non siamo lontani dall'avverarsi di un incubo: una botnet di smartphone che vengono costretti a chiamare a comando del malintenzionato di turno un numero a pagamento per scaricare suonerie e simílari, magari intestato a se stesso. Tuttavia pare che in tale evenienza non sarà molto difficile individuare la botnet e buttarla giù da parte degli operatori. Comunque sia, occhi aperti...





AL VIA IN SARDEGNA LA TELEVISIONE DIGITALE

Penserete che siamo impazziti, oppure che siamo entrati in qualche tunnel temporale che ci ha rimandato indietro nel tempo. Invece no, perché benché il digitale terrestre sia in circolazione ormai da diverso tempo, solamente dalla metà di ottobre in Italia c'è stato il passaggio ufficiale e definitivo dalle trasmissioni analogiche a quelle digitali, per quanto riguarda il territorio della Sardegna. La prossima regione a spegnere il segnale analogico sarà la Valle d'Aosta. Chi non ha ancora il decoder per il digitale terrestre farebbe bene a darsi una mossa, entro il 2012 tutta Italia sarà passata completamente in digitale.



GOOGLE "BRAIN TRAINER"

Pare che compiere ricerche su Internet aiuti a ringiovanire il cervello e a mantenerlo attivo. Lo studio è di alcuni ricercatori dell'Università della California ed è basato su 24 volontari tra i 55 e i 67 anni, dei quali la metà conosce e ha già esperienza su Internet. La ricerca sul Web occupa un'area del cervello maggiore in questi ultimi, e lo impegna più della lettura di un libro, mantenendolo quindi allenato e in forma. Una



FENNEC IN ANTICIPO

Già disponibile la prima release alpha di Fennec, il browser di Mozilla dedicato al mondo mobile. Doveva essere rilasciata verso dicembre, ma dato il buon punto di sviluppo in casa Mozilla hanno pensato di anticipare i test e quindi Fennec è già disponibile per il download. Anche se nasce come browser Web per dispositivi mobili (come il Nokia 810 Internet Table), Fennec può essere installato anche su sistemi desktop, ma in questo caso Mozilla non fornisce alcun supporto. Tra i problemi già conosciuti, il blocco intermittente dell'interfaccia durante il download di una pagina, la mancanza per il supporto dei plug-in e dei segnalibri e i lunghi tempi di rendering di alcune pagine. Secondo Mozilla la prima beta potrà essere disponibile già in dicembre, mentre la versione 1.0 potrebbe uscire già all'inizio del 2009.

I CYBORG SONO TRA NOI

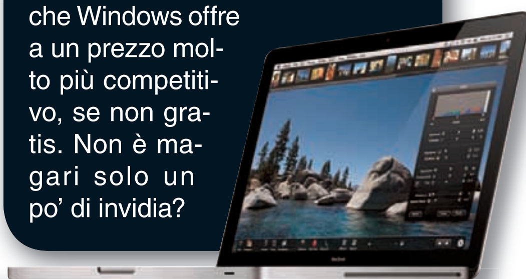
È il frutto dello studio di uno scienziato giapponese, Yoshiyuki Sankai, che ha dedicato tutta la vita alla robotica e alla cibernetica. Ciò che ha creato in realtà aiuterà molte persone nel lavoro o semplicemente ad avere una vita migliore, nel caso di perdita dell'uso degli arti.

Su YouTube (http://www.youtube.com/watch?v=ynL8BCXih8U) il video wche mostra lo strabiliante risultato ottenuto: Robot Suit HAL (Hybrid Assistive Limb) è un esoscheletro allo studio sin dal 1992 e che ora sta entrando nella fase di commercializzazione per conto di un'azienda fondata appositamente, la Cyberdyne (www.cyberdyne.jp). A causa dei costi ancora non può essere comprato ma solo affittato (e neanche a buon mercato), ma se le promesse verranno mantenute, non è da escludere che lo vedremo presto non solo negli ospedali specializzati, ma anche in industrie e cantieri dove aiuterà gli operai a compiere lavori pesanti. Siamo a un passo dalla fantascienza.

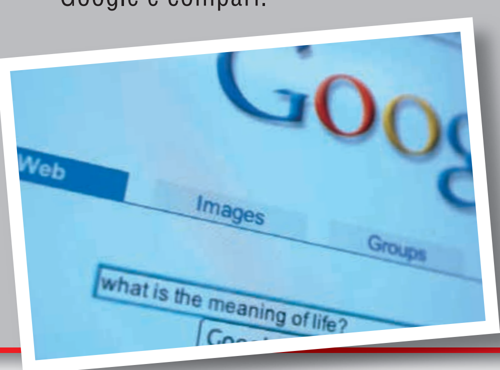


NUOVI MACBOOK MS CRITICA

Apple ha rinnovato la gamma MacBook con un re-styling che riporta alle origini: non più due colori plasticosi, ma un elegante chassis in alluminio che incorpora un display retroilluminato a LED protetto da vetro temperato e un touchpad di nuova concezione senza pulsante. Il prezzo è molto interessante, 1199 euro in Italia per la versione da 13,3" e 2 GHz. Nello stesso momento Microsoft si fa sentire con voci critiche nei confronti degli utenti che passano da Windows al mondo della mela morsicata. Secondo Brad Brooks, vicepresidente di Microsoft, chi passa al Mac invogliato dal prezzo concorrenziale si troverà in seguito a sborsare molti soldi extra per poter vivere la stessa esperienza che Windows offre a un prezzo molto più competitivo, se non gratis. Non è magari solo un po' di invidia?



buona notizia, dato che nessuno potrà più dire che ci stiamo rincitrullendo davanti al monitor. Con somma gioia di Google e compari.



NIENTE VISTA NEL MAINE

Che Vista a molti non piacesse è un dato di fatto. È un dato di fatto anche che le pubbliche amministrazioni spesso basano il proprio funzionamento su tecnologie abbastanza "datate", per non dire proprio obsolete. Per questo motivo lo stato americano del Maine ha siglato un accordo con Microsoft per garantirsi aggiornamenti e upgrade per le proprie macchine, che però esclude il passaggio a Windows Vista: troppe incompatibilità, sarebbe un aggiornamento inutile che non permetterebbe ai software scritti ad-hoc per funzionare su vecchi computer e su Windows 98 di continuare a girare e a servire i cittadini. Altro scacco per Microsoft.

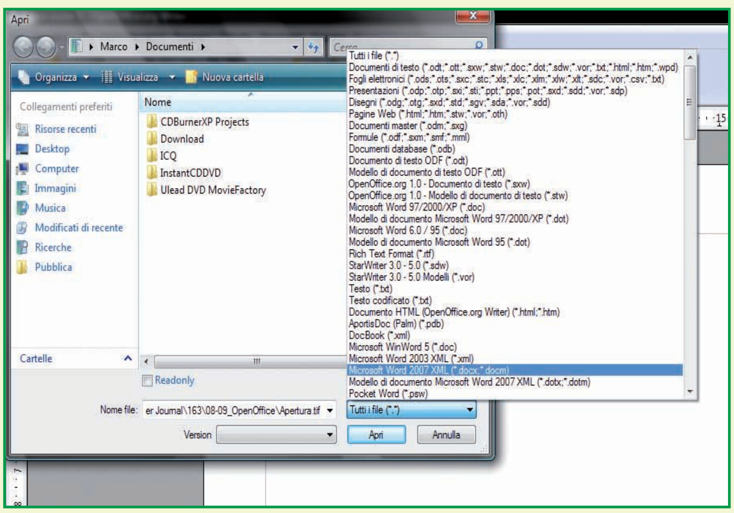


OpenOffice.org 3.0



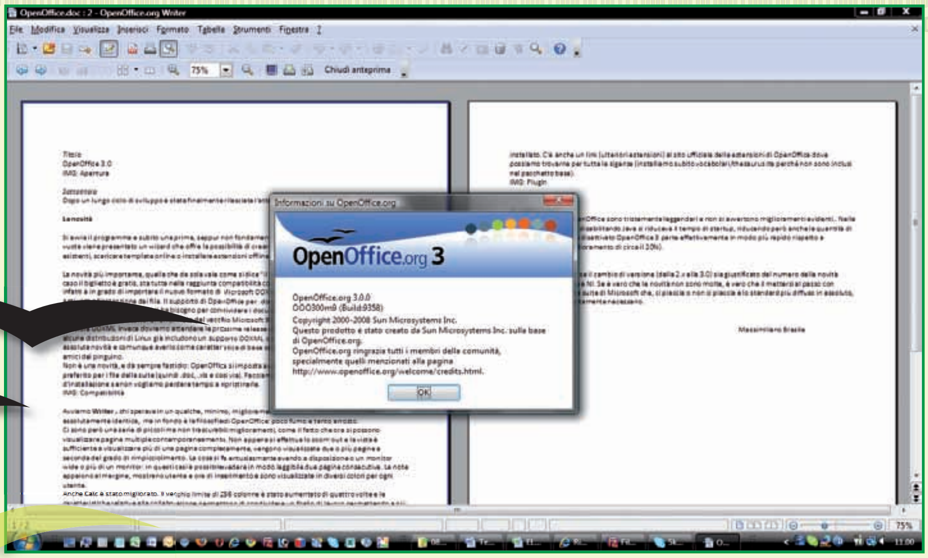
Dopo un lungo ciclo di sviluppo è stata finalmente rilasciata l'attesa nuova versione di OpenOffice

Si avvia il programma e subito una prima, seppur non fondamentale, novità: invece della solita finestra vuota viene presentato un wizard che offre la possibilità di creare diversi tipi di documenti, aprirne di esistenti, scaricare template online o installare estensioni offline e online. La novità più importante, quella che da sola vale come si dice "il prezzo del biglietto", anche se in questo caso il biglietto è gratis, sta tutta nella raggiunta compatibilità con Microsoft Office 2007. OpenOffice 3.0 infatti è in grado di importare il nuovo formato di Microsoft OOXML. Questo formato è riconoscibile per la x aggiunta all'estensione dei file. Il supporto di OpenOffice per .docx, .xlsx e .pptx è al momento in sola lettura, ma è tutto ciò di cui si ha bisogno per condividere i documenti con utenti di Office 2007 dal momento che si può salvare nel formato del vecchio Microsoft 97-2003. Per avere anche il supporto alla scrittura OOXML invece dovremo attendere le prossime release di aggiustamento. Per inciso va detto che alcune distribuzioni di Linux già includono un supporto OOXML con OpenOffice 2.4, ma su Windows è una assoluta novità e comunque averlo come caratteristica di base sarà un sensibile miglioramento anche gli per amici del pinguino. Non è una novità, e dà sempre fastidio: OpenOffice si imposta automaticamente come programma preferito per i file della suite (quindi .doc, .xls e così via). Facciamo quindi attenzione durante la procedura d'installazione se non vogliamo perdere tempo a ripristinarle.



Bisogna scorrere un po' l'elenco ma alla fine si trova.

Avviamo Writer , chi sperava in un qualche, minimo, miglioramento stilistico rimarrà deluso,l'interfaccia è assolutamente identica, ma in fondo è la filosofia di OpenOffice: poco fumo e tanto arrosto. Ci sono però una serie di piccoli ma non trascurabili miglioramenti, come il fatto che ora si possono visualizzare pagine multiple contemporaneamente. Non appena si effettua lo zoom out e la vista è sufficiente a visualizzare più di una pagina completamente, vengono vi-



sualizzate due o più pagine a seconda del grado di rimpicciolimento. La cosa si fa entusiasmante avendo a disposizione o un monitor wide o più di un monitor: in questi casi è possibile vedere in modo leggibile due pagine consecutive. Le note appaiono al margine, mostrano utente e ora di inserimento e sono visualizzate in diversi colori per ogni utente.
Anche Calc è stato migliorato. Il vecchio limite di 256 colonne è stato aumentato di quattro volte e le caratteristiche relative alla collaborazione permettono di condividere un foglio di lavoro permettendo a più utenti di lavorarci. Il proprietario potrà integrare i dati condivisi dopo averli controllati. Possono poi essere aggiunte delle barre d'errore personalizzabili.

:: I plugin

Come nelle versioni precedenti, anche OpenOffice 3.0 supporta le estensioni per aggiungere funzionalità ed alcune di quelle nuove, sviluppate esclusivamente per questa release, sono davvero utili. Una delle più interessanti è l'estensione per aprire ed editare i file .pdf (Sun PDF Import Extention). Una volta installata basta aprire il file .pdf in Writer, modificarlo a piacimento e riesportarlo in pdf senza alcuna perdita di qualità.
Pratico e veloce il gestore delle estensioni, disponibile nel menu Strumenti, che permette di installare le estensioni in modo davvero semplice: basta selezionare il file e il plugin che, previa conferma, viene installato. C'è anche un link (ulteriori estensioni) al sito ufficiale delle estensioni di OpenOffice dove possiamo trovarne per tutte le sigenze (installiamo subito vocabolari/thesaurus ita perché non sono inclusi nel pacchetto base).

:: Le performance

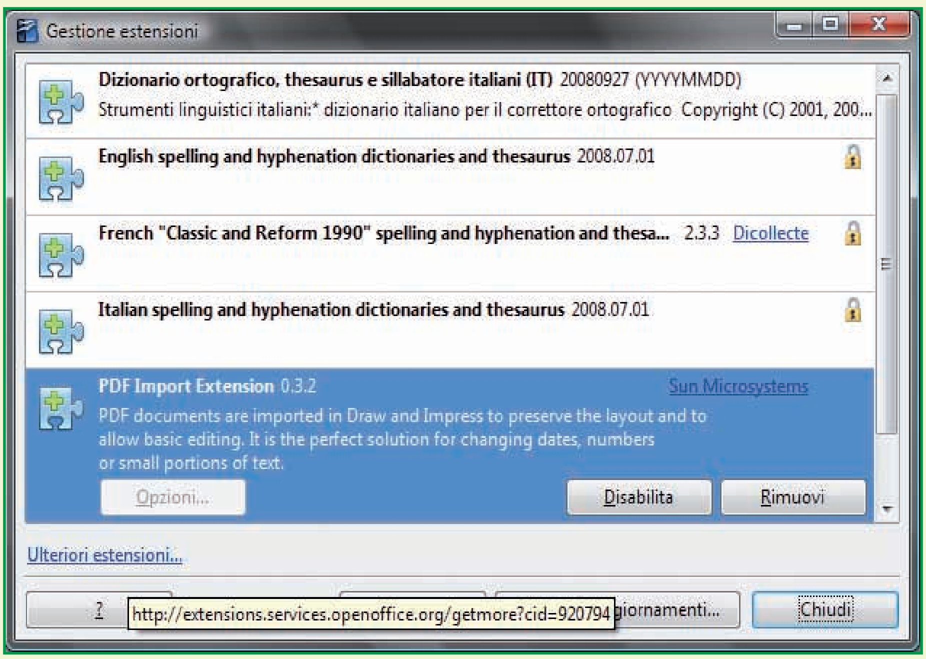
I tempi di avvio di OpenOffice sono tristemente leggendari e non si avvertono miglioramenti evidenti. Nella versione precedente, disabilitando Java si riduceva il tempo di startup, riducendo però anche la quantità di funzionalità. Con Java disattivato OpenOffice 3 parte effettivamente in modo più rapido rispetto a OpenOffice 2 (un miglioramento di circa il 20%).

:: Conclusioni

Se vi state chiedendo se il cambio di versione (dalla 2.x alla 3.0) sia giustificato dal numero delle novità introdotte, la risposta è NI.
Se è vero che le novità non sono molte, è vero che il mettersi al passo con l'ultima versione della suite di Microsoft che, ci piaccia o non ci piaccia è lo standard più diffuso in assoluto, è un passaggio assolutamente necessario.

Massimiliano Brasile

OpenOffice 3.0 ha alcune novità interessanti, tra cui il supporto ai formati di Microsoft Office 2007 e una nuova gestione dei plugin, ma ancora si porta dietro vecchi problemi, come l'avvio molto lento e l'invasiva associazione a se stesso delle estensioni documento di Office.



Il nuovo gestore dei plugin, facile e intuitivo.



Orwell 2008

È un dato di fatto: siamo tutti a rischio per quanto riguarda lo spionaggio delle nostre attività su Internet

Quello che infastidisce di più però è il fatto che a farlo siano quasi sempre soggetti mossi da interessi economici. Sempre più spesso trapelano notizie inquietanti su azioni di monitoraggio eseguite da società che non dovrebbero farlo, come nel caso di British Telecom, che addirittura viene beccata con le mani nel sacco mentre spia le attività dei suoi clienti inconsapevoli, qualcosa come 17 mila o 18 mila utenti.

:: Il campanello d'allarme

Tutto avveniva (e a quanto pare avviene ancora) in modo completamente nascosto per l'utente, che poteva solo notare che gradualmente i banner diventavano interessanti. Se ad esempio si erano visitati diversi siti che riguardano il birdwatching, apparivano magicamente pubblicità di binocoli, libri riguardo al riconoscimento dei pennuti e altro materiale sull'argomento.
Ma come fanno? Semplice: registrano e analizzano il traffico e cercano di conseguenza di proporre solo pubblicità di prodotti che l'utente potrebbe gradire e quindi comprare. Insomma, finiti i tempi dove un ragazzino di 10 anni riceve la pubblicità della nuova auto della BMW o il single proposte di viaggi da sogno per coppie!

:: Webwise

La società informatica Phorm, che ha creato il sistema Webwise, ribatte alle critiche di "spionaggio" avanzate da più parti, dichiarando che in realtà il nuovo sistema è una perla rara, perché permette agli utenti di navigare tra informazioni per loro interessanti. Insomma, "Cari Utenti, è vero che vi spiamo, ma lo facciamo per il vostro bene".
Ci siamo chiesti come funziona realmente questo sistema e abbiamo scoperto che funziona a due livelli: uno che può essere in qualche modo parzialmente limitato dagli utenti, mentre l'altro è completamente ingestibile.

:: Biscotti a colazione

Nel primo caso, siccome si utilizzano i cookie, qualcosa possiamo farla attraverso i settaggi del browser.

I cookie servono per salvare sul computer del visitatore di un sito determinate informazioni. In pratica sono un valore che il server chiede al client di conservare sull'hard disk del computer. Quando il server ne ha bisogno lo richiede al browser, che va a pescarlo tra i dati archiviati in locale e lo comunica al server. Ad esempio, se impostiamo il tema "Matrix" per un sito che permette questa personalizzazione, il nome del tema viene salvato in un cookie perché possa essere recuperato dal server come preferenza di personalizzazione nelle prossime visite. Se blocchiamo i cookie, il server non potrà più sapere che a noi piace il tema "Matrix" e visualizzerà il sito con il tema predefinito.



:: Biscotti avvelenati

Nel secondo caso, quello di Phorm, i cookie contengono altre informazioni: ad esempio categoria="elettronica" e gruppo="home video".

Il comportamento dell'utente viene annotato e conservato su uno specifico server insieme a indirizzo IP/ID, link visitato, cookie utilizzato, orario, giorno, link di provenienza e cose simili. In questo caso British Telecom ha installato sui propri server il sistema Phorm e quindi l'utente non ci scappa. La cosa si può riassumere in questo modo: scriviamo un indirizzo che vogliamo visitare ma in realtà la navigazione non segue quella strada. Il server che ci tiene collegati a Internet prende la richiesta del sito desiderato (per esempio www.pippo.com) e ci manda da tutt'altra parte, ma non si tratta solo di volgare redirect.

Questo è un sistema che ingannevolmente ci fa credere di essere collegati da un'altra parte: la nostra comunicazione viene mandata su un sito di Phorm, verosimilmente su webwise.net, con una stringa di comando simile a webwise.net/bind/?url=http://www.pippo.com.

A questo punto le nostre scelte vengono archiviate, dopo aver ricavato l'UserID dal nostro profilo su un apposito server. Tra l'altro la procedura di riconoscimento da parte del sistema di Phorm segue una strada un po' più contorta se abbiamo una linea di collegamento a Internet con IP dinamico, infatti nel caso di IP statico il riconoscimento è automatico (ecco perché sono sempre di più le offerte che comprendono uno o addirittura più IP statici).

Se non consentiamo i cookie (in certi casi è impossibile perché senza non possiamo accedere a moltissimi servizi), l'ISP ha dei problemi a identificarci ma comunque tutti i nostri movimenti sono registrati sul server dedicato. Avremo quindi una navigazione più protetta, ma solo fino a un certo punto.



:: In dettaglio

Facciamo un esempio pratico: vogliamo collegarci al sito www.pippo.com e guardiamo i vari passaggi.
Per semplicità, nell'esempio proposto, VEDO vuol dire quello che vediamo o che possiamo fare direttamente. MIOPC indica quello che avviene nel nostro PC senza il nostro intervento.
SERVER è quello che accade sui server dell'ISP.
LOCAL indicherà che il processo avviene in locale sul nostro PC mentre REMOTE che il processo avviene sui vari server.

Esempio di ISP onesto:

1) **LOCAL: VEDO**
Digito www.pippo.com sul mio browser perché voglio visitare questo sito.

2) **LOCAL: MIOPC**
Il browser controlla che non ci siano cookie sul disco associati al sito www.pippo.com. Il mio computer invia la richiesta al server ISP per il dominio pippo.com.

3) **REMOTE: SERVER ISP**
Il server dell'ISP inoltra la richiesta al server del dominio pippo.com.

4) **LOCAL: VEDO**
Vedo la pagina di www.pippo.com.

Esempio di ISP che usa i prodotti Phorm:

1) **LOCAL: VEDO**
Digito www.pippo.com sul mio browser perché voglio visitare questo sito.

2) **LOCAL: MIOPC**
Il browser controlla che non ci siano cookie sul disco associati al sito www.pippo.com.
Il mio computer invia la richiesta al server ISP per il dominio pippo.com.

3) **REMOTE: SERVER ISP**
Il server dell'ISP, opportunamente guidato dal software Webwise, controlla che ci sia l'associazione tra il cookie di Webwise.net e il dominio pippo.com.

4) **REMOTE: SERVER ISP**
Se il dominio non è presente nella lista il server blocca l'accesso al sito www.pippo.com e risponde con l'errore "307 Tempory Redirect" facendo credere al browser che si tratti sempre di www.pippo.com ma momentaneamente trasferito su un altro computer.

5) **LOCAL: MIOPC**
Il mio browser è convinto che ci sia stato un trasferimento momentaneo e quindi invia al sito www.webwise.net la richiesta di prima, più eventuali cookie presenti per il dominio pippo.com.

6) **REMOTE: SERVER ISP**
Se non viene trovato alcun cookie per pippo.com allora il sistema ne crea uno e usando lo stesso trucchetto dice ancora al mio browser che c'è stata una nuova redirect a un falso www.pippo.com.

7) **LOCAL: MIOPC**
A questo punto il mio browser fa l'unica cosa che può fare e manda un'altra richiesta al finto www.pippo.com presente solo sul server dell'ISP.

8) **REMOTE: SERVER ISP**
Il server bugiardo dice di essere www.pippo.com e comunica ancora che c'è stato il solito errore 307 e questa volta rimanda il povero browser all'indirizzo del vero www.pippo.com, lasciando a lui la gestione, ma non senza aver inviato un bel biscottino al mio browser, in cui è stato salvato il nuovo UID che il sistema mi ha appena attribuito. Il browser naturalmente penserà che questo cookie fa parte del dominio pippo.com mentre invece non c'entra niente: infatti il sito non l'abbiamo neppure visto. Intercetta poi i cookie, uno per il dominio target reale e uno camuffato che invece viene richiesto



Questo signore, Kent Ertugrul, Chief Exectuve Officer di Phorm, ci spia per il nostro "bene". E se qualcono spiasse lui?

e usato da Webwise.net. Quindi il cookie camuffato di Webwise.net viene tolto dalla coda della query, come strategia per rimanere il più possibile "nascosti". Questo cookie potrebbe anche rimanere in coda, visto che un sito che non sia configurato per leggere e usare i cookie di Webwise.net, magari per dare fastidio a Phorm in qualche modo losco, difficilmente potrebbe utilizzarlo. Ma alla Phorm non sono affatto stupidi e ci stanno attenti.

9) **REMOTE: SERVER ISP (SERVER DATABASE)**
Ora il software di Phorm intercetta la mia query di ritorno da www.pippo.com e una copia delle informazioni, inclusi tutti e due i cookie, viene inviata a un altro server che si occupa della gestione di un enorme database. Lì viene salvata per creare un mio accurato identikit digitale.

10a) **LOCAL: VEDO**
Vedo la mia pagina mentre in contemporanea accade la situazione 10b di cui io sono del tutto ignaro

10b) **REMOTE: SERVER ISP (SERVER DATABASE)**
Il server che gestisce il database cerca nella pagina di www.pippo.com possibili informazioni (argomenti, prodotti venduti e cose simili) che verranno aggiunte nel mio profilo per delineare le mie preferenze.

:: Casi estremi

Il fatto di essere osservati potrebbe sembrare non particolarmente seccante, ma ci sono delle cose da prendere seriamente in considerazione. Ammettiamo che a Londra ci sia un quartiere X che ha un alto tasso di abitanti italiani. British Telecom, oltre ad avere una UserID per ogni contratto telefonico con IP fisso, grazie a Phorm conosce a menadito tutte le abitudini degli utenti del quartiere. Poniamo il caso che un imprenditore voglia aprire un negozio di moda francese nel quartiere X. Contemporaneamente un altro imprenditore vuole fare la stessa cosa ma con tema italiano. Tutti e due vanno in banca e chiedono un finanziamento. La banca, accedendo alle informazioni sul quartiere X fornite da Phorm, potrebbe decidere di dare il finanziamento con tasso minore all'italiano e maggiorarlo a causa del rischio di flop al francese.
Altro caso ipotetico: se visitiamo spesso siti che riguardano sport estremi come paracadutismo o simili, che le assicurazioni non vogliono coprire se non con speciali polizze, ci potremmo trovare un aumento del premio immotivato. Addirittura, si può verificare la stessa cosa se il titolo della nostra ricerca scolastica è "Le malattie cancerogene e le varie percentuali di guarigione che si possono ottenere con i sistemi moderni": l'assicurazione ottiene da Phorm le informazioni sulla nostra ricerca sul Web e i nostri genitori si vedono aumentare il premio o addirittura annullare la polizza.

LA PROVA DEL NOVE

Se volete togliervi il dubbio o offrire il servizio di controllo sulla vostra pagina Web potete inserire questo pratico codice in Javascript, che riconosce se vi siete beccati Webwise:

```
<script type="text/javascript">
function hasPhormCookie()
{
var found = false;
var c = document.cookie
if (c.length>0)
      {
      if (c.indexOf("webwise=", 0)>-
1)
              {return found=true;}
      }
}

if (hasPhormCookie()==true)
      {document.write("Phorm ti sta
spiando")}
      else
      {document.write("Phorm non ti
sta spiando");}
</script>
```

:: Quale soluzione?

Anche usare un proxy anonimo può essere uno svantaggio per l'utente: se blocchiamo i cookie e usiamo un proxy anonimo, il sistema segue comunque tutti gli spostamenti tracciando i percorsi che effettuiamo. Infatti il proxy consente di essere anonimi rispetto al sito di destinazione e non certo agli occhi del nostro ISP che può benissimo archiviare i dati in base alle richieste che giungono dal nostro computer, soprattutto se usiamo un IP fisso. Questo, se da una parte porta il vantaggio dell'anonimato rispetto il sito di destinazione (ammesso che non faccia parte del sistema Webwise), dall'altra ci rende la navigazione più lenta e macchinosa. Vale la pena?



Si potrebbe usare un punto d'accesso pubblico per quello che noi riteniamo operazioni delicate. Questo rimane in realtà l'unica soluzione valida a patto che si tratti di punti d'accesso wireless che non richiedano una qualche registrazione. Oppure usare computer in modalità remota in un altro luogo, possibilmente che non sia sotto un ISP che usa i sistemi di tracciamento degli utenti. Altre opzioni sono quelle di usare collegamenti in VPN o SSL. Ricordiamoci che anche le e-mail sono un potenziale veicolo di informazioni per un ISP malintenzionato: le e-mail andrebbero tutte criptate. Un altro semplice accorgimento potrebbe essere quello di impostare il browser per bloccare i cookie di Webwise.net.



Chat (in)sicure



Teniamo segreti i nostri... segreti

Siamo nella nostra stanza d'albergo o in un'area di sosta, accendiamo il fido notebook e controlliamo la disponibilità di un accesso a Internet wireless gratuito. La fortuna ci assiste e riusciamo ad agganciare un bel segnale, forte e disponibile.
Lanciamo il nostro client di instant messaging. Tutto a posto, sembrerebbe; ma è davvero così? Si tratta di paranoia, oppure esiste la possibilità che qualcuno stia ficcando il naso in questioni che non lo riguardano intercettando le comunicazioni tra il nostro pc e l'access point? E, se questa possibilità esistesse realmente, possiamo in qualche modo difenderci da antenne indiscrete? Per capire meglio se e come qualche curiosone possa essere in grado di carpire qualche segreto dall'etere e quali contromisure mettere in atto, è utile ripassare i concetti fondamentali delle comunicazioni dati senza filo.

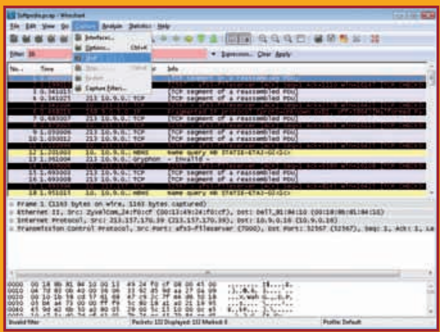


WI-FI in dettaglio

Con il termine WiFi si è soliti indicare tutta una serie di dispositivi che possono connettersi a delle reti locali senza fili (WLAN) sfruttando lo standard IEEE 802.11. Il medesimo consorzio ha sviluppato sia le derivazioni 802.11a, b e g sia gli standard di sicurezza WEP, WPA e WPA2.
Trattandosi di emissioni in radiofrequenza, ovviamente esiste la possibilità che il segnale possa raggiungere dispositivi che non sono i reali destinatari della nostra trasmissione; come è facilmente intuibile, senza un meccanismo di protezione della connessione e qualche forma di crittografazione dei dati, è abbastanza semplice "ascoltare" una conversazione di questo tipo. A maggior ragione considerando che gli applicativi di uso comune (client di posta elettronica, ftp, browser, instant messenger ecc.) di default trasmettono i dati in chiaro. Come fare a essere ragionevolmente certi di non spifferare ai quattro venti i segreti delle nostre conversazioni?

:: Connessione sicura

Iniziamo dall'aspetto relativo alla connessione con l'access point. Più che avere delle perplessità sul tipo di autenticazione utilizzata, iniziamo con il chiederci se si tratti effettivamente di un vero access point pubblico e non piuttosto di un altro dispositivo che stia facendo credere



I programmi Sniffer sono freeware e semplici da trovare. Poca spesa e tanta

di essere qualcosa che non è. Non è molto difficile configurare un dispositivo dotato di interfaccia wireless per ingannare un utente; il modo più semplice è coprire con le proprie emissioni l'access point "ufficiale" utilizzandone il medesimo SSID e costringendo il sistema operativo del computer vittima a connettersi a quello che sembrerebbe in tutto e per tutto l'access point "ufficiale". Teniamo inoltre presente che alcuni sistemi operativi aggiornano la lista delle reti disponibili ogni volta che viene rilevata una rete non protetta, aumentando quindi la possibilità di essere ingannati. Inoltre, se il punto di accesso "clonato" non prevede meccanismi di autenticazione, non esistono metodi di prevenzione semplici ed efficaci al 100%. Nel dubbio, quando ci colleghiamo a una rete wireless pubblica, presumiamo sempre di essere in una situazione a rischio e prendiamo le uniche precauzioni affidabili sotto il nostro controllo: il settaggio corretto delle applicazioni che scambiano dati.

:: WEP, WPA, ecc...

Il Wired Equivalent Privacy (WEP) è parte dello standard IEEE 802.11 (ratificato nel 1999) e in particolare è quella parte dello standard che specifica il protocollo utilizzato per rendere sicure le trasmissioni radio delle reti WiFi. WEP è stato progettato per fornire una sicurezza comparabile a quelle delle normali LAN basate su cavo. Seri difetti sono stati scoperti nella particolare implementazione dell'algoritmo crittografico utilizzato per rendere sicure le comunicazioni. Questo ha reso necessario una revisione del WEP che adesso viene considerato un sottoinsieme del più sicuro standard WiFi Protected Access (WPA) rilasciato nel 2003 e facente parte dell'IEEE 802.11i (conosciuto come WPA2) definito nel giugno del 2004. IEEE 802.11i (conosciuto anche come WPA2) è uno standard sviluppato dalla IEEE specificamente per fornire uno strato di sicurezza alle comunicazioni basate sullo standard IEEE 802.11. Prima dello standard 802.11i la WiFi Alliance aveva introdotto il WiFi Protected Access (WPA) un sottoinsieme delle specifiche 802.11i. Il WPA era stato introdotto per tamponare l'emergenza sicurezza dovuta al WEP e rappresenta solamente uno standard transitorio mentre l'802.11i veniva terminato e perfezionato. La WiFi Alliance ha deciso di chiamare le specifiche 802.11i con il nome di WPA2 per rendere semplice all'utente comune l'individuazione delle schede basate sul nuovo standard. L'802.11i utilizza come algoritmo crittografico l'Advanced Encryption Standard (AES) a differenza del WEP e del WPA che utilizzano l'RC4.

:: Come difendersi

Il primo passo è quello di scegliere con attenzione i nostri strumenti ovvero preferire quelle applicazioni che consentono di crittografare in maniera più o meno complessa ed efficace i nostri dati sensibili. Molta attenzione



In un unico instant messenger possiamo raggruppare tutti i nostri amici che utilizzano programmi differenti.

anche agli add-on che implementano la crittografia nelle applicazioni scelte, anche sui file transfer che possono avvenire durante una sessione di chat. Tra i vari client di messaging disponibili, scegliamone uno open source che offre un controllo pressoché totale sull'operato del client stesso. Se vogliamo il massimo della interoperabilità, esistono anche client che si connettono a server Jabber i quali dispongono di un sistema di transport in grado di interfacciarsi con i servizi più comuni semplificando ulteriormente la vita all'utente.

Gian Franco Baroni

JABBER

Jabber è un insieme di protocolli aperti di messaggistica istantanea e presenza basato su XML. Il software basato su Jabber è diffuso su migliaia di server disseminati su Internet ed è usato da oltre dieci milioni di persone in tutto il mondo, secondo la Jabber Software Foundation. Una caratteristica unica del sistema Jabber è quella dei transport, anche conosciuti come gateway o agenti, che consentono agli utenti di accedere a reti che usano altri protocolli, come AIM e ICQ (usando il protocollo OSCAR), MSN Messenger e Windows Messenger (usando il Servizio Messenger .NET), Yahoo! Messenger, SMS o Email. A differenza dei client multiprotocollo come Trillian o Pidgin, Jabber fornisce questo accesso a livello di server, comunicando per mezzo di servizi speciali gateway che girano su un computer remoto.



GLI ZOMBIE DI FACEBOOK

Hanno usato il più famoso sito di social networking per creare una botnet

Sappiamo tutti cos'è una botnet: una rete di "bot", cioè di computer zombie che, possibilmente a loro insaputa, agiscono sotto il controllo di un hacker per compiere un particolare compito sulla rete, normalmente un attacco verso un server. Va da sé che maggiore è il numero di questi computer, maggiori sono le possibilità per l'hacker di raggiungere in breve tempo il proprio scopo. Dato per accertato il fatto che l'hacker stesso sappia cosa sta facendo e che il software che ha scritto esegua alla perfezione il proprio compito su ogni singolo computer, il problema principale diventa non più come infettare una macchina prendendone il controllo, ma come infettarne il maggior numero possibile per aumentare le probabilità di successo.

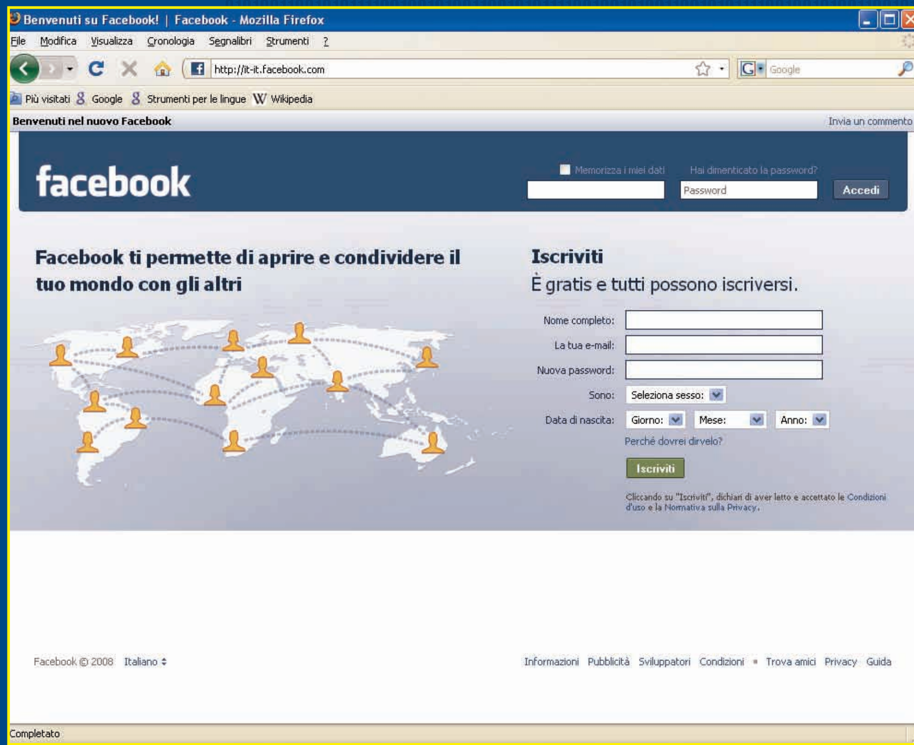


Sembra incredibile ma c'è ancora chi ci casca e scarica tutto quello che gli arriva dalla Rete.

I sistemi sono sempre più numerosi e fantasiosi: si può creare una pagina maligna in un sito che sfrutta le falle di sicurezza di Internet Explorer per installare un trojan sul computer del visitatore, oppure inviare un programmino dalle apparenze innocue via mail o via istant messenger (come fa l'ormai tristemente famoso MSN virus con il file photo.zip), insomma, tanti modi per giungere a un solo scopo: fare in modo che il maggior numero di navigatori incauti cadano nella trappola come bei pescioni.

Va da sé che i siti di social networking

siano una ghiotta occasione per accedere al più ampio numero possibile di candidati a bot. E poiché “faccia da libro” è quello che di questi tempi va per la maggiore, ecco che uno smanettone greco ha pensato di verificare la possibilità di usarlo per far eseguire compiti da botnet ai computer degli iscritti a Facebook senza che questi se ne accorgano e senza installare alcun programma su di essi. Le possibilità di un attacco di questo tipo sono limitate e non troppo invasive, sostanzialmente si riducono a un tentativo di DoS verso un qualunque server; va detto anche che attacchi di questo tipo sono facilmente superabili da parte dell’amministrazione del sito semplicemente cambiando un po’ le carte in tavola. Ma questo ci interessa poco, a noi interessa capire come funziona Facebook e come sia stato possibile tentare un attacco di questo tipo usando solo ciò che il sito stesso mette a disposizione.



L’articolo prende spunto da Facebook, ma il principio si applica anche ad altri siti con caratteristiche simili, come MySpace.

:: “Questa è Struttura”...

...come diceva il buon vecchio Morpheus allo spaesato Neo. “Possiamo caricare di tutto: vestiti, equipaggiamento, armi, addestramento simulato...”.

E un po’ Facebook assomiglia a Struttura: abbiamo un bel contenitore in cui sono presenti alcuni elementi di base, che costituiscono il profilo principale di un iscritto, che possiamo riempire di applicazioni utili a favorire l’interazione tra gli utenti e la costituzione di gruppi di utenti legati da amicizia, interessi comuni e anche rapporti di lavoro. Alcune di queste applicazioni sono proposte direttamente dagli sviluppatori di Facebook, ma le modalità e le API per scrivere applicazioni proprie sono disponibili in un’area apposita, a beneficio di chi voglia costruirne una in base ai propri interessi da condividere con altre persone. Naturalmente non basta accedere all’area di programmazione e mettere insieme quattro elementi predefiniti per costruire un’applicazione: occorre saper programmare in PHP, avere a disposizione un server su cui ospitare la propria applicazione e ovviamente sottoscrivere le norme sulla buona condotta, sulla riservatezza dei dati e tutto il solito blablabla legale cui siamo abituati.
L’applicazione costruita verrà poi integrata nel profilo degli utenti che decideranno di includerla, in modo che i loro amici/colleghi/visitatori possano usufruirne, includerla a loro volta o semplicemente vederne gli effetti sul profilo visitato (ne è un esempio l’applicazione Smiley, con cui viene visualizzata una faccina corrispondente al proprio umore sul profilo di chi la include).
Le modalità di integrazione della nostra applicazione nel profilo di un iscritto sono due: usando FBML (Facebook Markup Language, il linguaggio simile all’HTML usato da Facebook per la scrittura di sempli-





L'applicazione in questione è ancora attiva su Facebook: per raggiungerla l'indirizzo è http://www.facebook.com/apps/application.php?id=8752912084.

ci applicazioni) oppure inviando l'output del nostro codice PHP direttamente in un IFRAME. Tralasciando, per questa volta, ciò che implica dal punto di vista della sicurezza la presenza di un IFRAME in una pagina Web, vediamo più in dettaglio come è stata sviluppata l'applicazione nei suoi elementi principali e, per arrivare al succo del discorso, come può essere usata per costituire l'ipotetica botnet e come questa potrebbe essere usata per creare problemi sulla rete.

:: Le immagini nascoste

Il primo passo è stato quello di creare un'applicazione che mostra ogni giorno una foto diversa del National Geographic (che non ha niente a che vedere con la faccenda) sul profilo dell'utente che l'ha integrata. Conosciamo tutti la qualità e la bellezza di queste foto, quindi è stato anche abbastanza facile trovare una discreta base di utenti pronti a costituire (inconsapevoli) la botnet virtuale. L'applicazione visualizzata sul computer degli utenti, però, non si limita a questo: ogni volta che essi si connettono al proprio profilo, parte una richiesta verso un altro server per il download di tre grosse foto, le quali però non vengono mai visualizzate.

Si tratta in sostanza di tentare di raggiungere la saturazione della banda del server in questione, causandone la dipartita momentanea dal Web. Detto in poche parole, un DoS arrecato senza infettare le macchine altrui, che continuano ignare a funzionare immutate come sempre. Nel caso in questione l'attacco è stato solo un test per dimostrare la vulnerabilità di Facebook e il server "vittima" era gestito da chi ha lanciato l'attacco, quindi non è stato arrecato danno ad alcun server reale.
Ma come si fa a includere in una pagina immagini che non vengono mai visualizzate?
Giusta obiezione. Tra i vari metodi, probabilmente i più semplici sono la presenza di una funzione di preload scritta in Javascript e l'uso di una particolare proprietà dei fogli di stile.



:: Preload_Images()

Il preload delle immagini viene usato spesso nelle pagine che vogliono mostrare un rollover quando il visitatore interagisce con un elemento delle stesse. Ad esempio, passando il puntatore su un pulsante questo cambia colore: si tratta di due immagini, una mostrata e una precaricata e mostrata solamente quando il puntatore passa sopra l'area dell'elemento pulsante, sostituendo l'immagine precedente. Esistono numerosi script sul Web che illustrano questa tecnica, Photoshop stesso permette di creare immagini e codice necessario per l'effetto rollover, ma in sostanza tutti fanno uso degli eventi OnMouseOver e OnMouseOut degli elementi HTML. Prima carico le immagini secondarie e le memorizzo per un uso successivo, poi con OnMouseOver posso rilevare quando il puntatore passa sull'oggetto (e quindi mostrare la seconda immagine precaricata), mentre con OnMouseOut rilevo l'uscita del puntatore dall'area dell'oggetto (e ripristinare l'immagine precedente). Ma se noi precarichiamo le immagini e poi non le usiamo?
Abbiamo ottenuto il nostro scopo: inseriamo il preload nella nostra applicazione Facebook (naturalmente si tratterà del preload di immagini abbastanza consistenti, non certo le piccole GIF di un pulsantino), non ci curiamo di gestire gli eventi OnMouseOver e OnMouseOut e attendiamo che migliaia di utenti installino l'applicazione e inviino a loro insaputa migliaia di richieste al server che ospita le grosse immagini che, prima o poi, andrà giù per il traffico generato.

:: L'alternativa dei CSS

Il secondo sistema utile allo scopo non va a scomodare Javascript e si limita a usare i fogli di stile. Innanzitutto occorre preparare una classe per gli oggetti immagini (naturalmente da usare solo per le nostre immagini fantasma), la quale contiene solamente la proprietà display:none; e niente altro. Poi, in un punto qualsiasi del codice HTML

```
<SCRIPT language="JavaScript">
    <!--

    if (document.images)
    {
      preload_image_object = new Image();
      // set image url
      image_url = new Array();
      image_url[0] = "http://mydomain.com/image0.gif";
      image_url[1] = "http://mydomain.com/image1.gif";
      image_url[2] = "http://mydomain.com/image2.gif";
      image_url[3] = "http://mydomain.com/image3.gif";

       var i = 0;
       for(i=0; i<=3; i++)
         preload_image_object.src = image_url[i];
    }

    //-->
</SCRIPT>
```

Una semplice funzione di precaricamento delle immagini in Javascript: ovviamente senza la gestione degli eventi mouse diventa una sanguisuga per la banda...

```
<style type="text/css">
.hiddenPic {display:none;}
</style>

.
.
.

<img src="img01.jpg"
  alt="Immagine nascosta 1" title="Immagine nascosta 1"
    height="350" width="350" class="hiddenPic">

<img src="img02.jpg"
  alt="Immagine nascosta 2" title="Immagine nascosta 2"
     height="350" width="350" class="hiddenPic">

<img src="img03.jpg"
  alt="Immagine nascosta 3" title="Immagine nascosta 3"
     height="350" width="350" class="hiddenPic">
```

Ecco invece come includere immagini nascoste senza usare Javascript: se nulla le rende visibili cambiandone lo stile, verranno caricate per niente.

che verrà visualizzato in Facebook, inseriamo le immagini dichiarandole con il nostro stile "fantasma".
In questo modo le immagini non verranno visualizzate nel browser dell'ignaro utente che decida di integrare al proprio profilo la nostra applicazione, e il gioco è fatto.

:: Può funzionare?

Potrebbe: il condizionale è d'obbligo, visto che in questo caso si è trattato solo di uno studio e non di un'applicazione reale. Potrebbe perché, alla velocità delle connessioni Internet di oggi, scaricare qualche centinaio di Kbyte in più è assolutamente trasparente all'utente ignaro, che non si accorgerebbe di niente se non di un lieve ritardo nella visualizzazione della schermata di Facebook. Potrebbe, perché un malintenzionato con un po' di fantasia ha sicuramente modo di studiare un'applicazione Facebook che attiri moltissime persone (in questo caso si è raggiunto il migliaio di persone, del tutto insufficienti per poter causare veri problemi sulla rete) creando di conseguenza una botnet di adeguate dimensioni. Ma la cosa più preoccupante è il fatto che i responsabili di Facebook minimizzino la questione asserendo che "chi mai sprecherebbe tempo e risorse per cercare di usare il nostro sistema solo per tirar giù un sito Web? Perché mai se invece potrebbe trarre beneficio e guadagnare soldi attraverso gli annunci pubblicitari usando la sua applicazione?". Ciò significa che nulla è stato fatto per impedire che le applicazioni Facebook escano dal dominio e restino invece ben confinate senza arrecare danni ad altri? Staremo a vedere: di certo questo è la punta dell'iceberg che vedrà Facebook (ed altri sistemi simili) presi di mira per un po' da hacker di tutti i tipi e di tutti i livelli di esperienza.

PROGRAMMARE PER FACEBOOK



Facendo clic su Sviluppatori, nella home page di Facebook, si accede all'area in cui sono contenute tutte le informazioni a proposito della programmazione di nuove applicazioni per il sistema. Sono presenti anche diversi strumenti per il test e per la pubblicazione delle applicazioni. Un'ampia sezione wiki costantemente aggiornata costituisce il punto di partenza per tutti quelli che desiderano capire nel dettaglio il sistema di programmazione per Facebook e vogliono prendervi parte.



Come mosche nella tela del ragno

Come funziona oggi il crimine informatico secondo chi lo combatte per mestiere

Eugene Kaspersky è una persona che, oltre a combattere per mestiere virus e malware con il proprio software, ha anche deciso di far sentire la sua voce, rilasciando al pubblico un breve articolo sulle sue vedute e sulle sue proposte per migliorare la situazione attuale.

:: Analisi del dato di fatto

Ancora oggi, a più di ventíanni dalla loro comparsa, i virus si diffondono e causano danni e scompiglio in ampie proporzioni; eppure... tutto prosegue indisturbato, se oggi sconfiggo un malware domani un altro tenterà di entrare nel mio PC, chi sta dietro, dallíaltra parte, continua a fare soldi alle spese degli "utenti normali" (a questo punto il termine "zombie" è più che appropriato) e, a dispetto delle tante operazioni delle forze dellíordine, il problema non è stato nemmeno scalfito. In più, il successo è talmente facile da raggiungere che il modello del business tradizionale e legale lo si applica tranquillamente anche al crimine informatico. Tutto sommato la solfa è la stessa: io ho qualcosa che ti serve e te la vendo, tu poi ci fai soldi usandola a tuo vantaggio.

> **"L'individuo o il gruppo che possiede una botnet capace di lanciare attacchi DDoS o di distribuire spam, ad esempio, ha bisogno di indirizzi e-mail cui inviare i messaggi. Qualcun'altro, con cui il proprietario della botnet è in contatto, verrà incontro a questa esigenza rubando e vendendo liste di indirizzi. Questo modello di business copia, di fatto, quello del commercio lecito."**

:: Perché lo fanno?

Soldi: principalmente il motivo è fare soldi con fatica poca o nulla e alle spalle di chi ci casca. Ne sono prova le cifre divulgate dalle autorità quando vengono pescati truffatori e criminali informatici nel corso delle operazioni: si parla di centinaia di migliaia di euro o di dollari, con punte che arrivano a milioni. Lo fanno perché è facile, ormai gli strumenti circolano quasi liberamente nel mercato underground, non devo più scrivermi il software da solo perché spendo un poí di soldi e me lo danno già fatto (e con quello ovviamente ci creo la

mia botnet e tiro su bei soldoni). Sono stati scoperti strumenti appositi, con la loro interfaccia Web intuitiva e immediata, addirittura in certi casi presente nel malware installato nei computer delle vittime e a cui il cattivone di turno accede comodamente dal proprio browser.
Lo fanno perché difficilmente si viene beccati con le mani nel sacco, e anche chi viene beccato non fa numero, sono talmente pochi che possono tranquillamente fare da capro espiatorio per tutti gli altri. E lo fanno anche perché le nuove tecnologie glielo permettono: pensiamo per esempio al Web 2.0, con tutte queste nuove applicazioni, sulle quali si basano altre applicazioni, le quali poi mettono a disposizione librerie per nuove applicazioni e cosÏ via... Basta un piccolo baco alla fonte per generare un potente effetto valanga che coinvolge tutto ciò che è stato fatto basandosi su quel lavoro.
Nulla ne è immune: home banking, giochi online, servizi vari, social networking eccetera, basta una piccola distrazione per aprire le porte a questi loschi figuri (ma spesso la parte più grande della colpa spetta proprio alle vittime stesse). Naturalmente, chi fa del crimine informatico la propria filosofia di vita è di base un approfittatore che sa cogliere al volo queste occasioni.

Il criterio cardine alla base di ogni business è senza dubbio il profitto, e il crimine informatico non fa certo eccezione: esso è estremamente redditizio.



Pannello di controllo di una botnet visto da un hacker.

:: Il manuale del giovane truffatore

Sono due gli aspetti principali che i criminali informatici devono tenere presenti nel loro operato. Per prima cosa, la "consegna" del malware nel computer della vittima (Delivery). Devono tener conto dei sistemi di sicurezza esistenti e trovare il modo di passare inosservati, di non essere rilevati dai software antivirus e dagli strumenti delle forze dell'ordine. Un po' come un elefante che tenta di entrare in un negozio di preziose porcellane, basta un attimo per far suonare il campanello d'allarme (salvo poi scoprire che le porcellane invece sono fatte di gomma e non si rompono cadendo, et voilà, il nostro computer è infettato a dispetto dei 10 programmi antivirus, firewall e anti-malware che abbiamo installato). Una volta entrati, si devono preoccupare che il malware sopravviva il più possibile (Deployment). Ogni volta bisogna trovare un sistema nuovo per non essere rilevati dai sistemi di sicurezza o per lo meno non esserlo il più tardi possibile, per dare modo al malware stesso di attivarsi e portare a termine il proprio compito. Le tecniche sono varie (in realtà queste persone sono sempre alla ricerca della pietra filosofale di tutti i malware), come le tecniche di polimorfismo in voga negli anni 90 o i packer e crypter di tutte le forme e di tutti i colori. Addirittura il server maligno stesso ricompila il codice del malware ogni 5 minuti per cambiarne forma e firma per essere il più possibile nuovo e invisibile..

"Fondamentalmente, l'efficacia di qualsiasi sistema di sicurezza dipende dall'anello più debole del sistema. Nel caso della sicurezza online, l'anello più debole è rappresentato dal fattore umano. Oggi, le tecniche di ingegneria sociale sono un elemento chiave nel processo di diffusione del malware."

:: Quindi che si fa?

Mai abbassare la guardia, né l'utente finale né chi deve vigilare perchè non vi siano rischi di sicurezza. È inutile il più moderno antivirus se non si sa come usarlo e come tenerlo aggiornato. Il guaio è che gli utenti sprovveduti sono troppi per poter implementare una politica di sicurezza diffusa ed efficiente. La colpa è dell'eccessivo consumismo tecnologico, si "forza" il pubblico a comprare computer e connessione ma lì finiscono le responsabilità, poi sono affari "dell'utonto" usarli in sicurezza. Il risultato è che adesso si tenta di correre ai ripari con delle pezze qua e là, inutili quando è alla base che il sistema non funziona. Occorre una più ampia alfabetizzazione informatica, dice Kaspersky, che offra a tutti le conoscenze e gli strumenti per evitare di cadere nel tranello o, per restare in tema di Web, nella tela del ragno. Come tante mosche.

Privateer



Io cripto da solo

Scriviamo il nostro programma per criptare i file

Da quando l'uomo ha iniziato a comunicare informazioni, ha anche sentito l'esigenza di proteggerle.
Dalle complicate tavole e tabelle dell'era pre informatica, passando per le prime macchine di cifratura elettromeccaniche come la famosa Enigma della Germania nazista, i sistemi si son fatti via via sempre più complessi.
Oggi sono molti quelli di cifratura pubblici, noti ormai da anni, come ad esempio il mitico Blowfish ma, appunto, sono pubblici e noti. Ciò che ci interessa studiare è il principio della cifratura stessa per arrivare a produrre un sistema da noi elaborato. Se il suo principio è piuttosto semplice, come si vedrà utilizzeremo codice in VbScript facilmente convertibile in altri linguaggi, ha un grosso vantaggio: non lo usa nessuno.
Il nostro obbiettivo è il seguente: archiviare dei dati testuali in un database Access senza che questi dati siano visibili da chi poi decida di aprirlo in modo non autorizzato.

:: Primo passo

Poniamo il caso che la codifica venga legata a una parola chiave fissa di 6 caratteri ASCII standard.
Il nostro programma verrà quindi diviso in tre grossi blocchi logici. Il primo blocco conterrà la parte relativa alla codifica e decodifica dei caratteri, mentre gli altri due conterranno il codice relativo alla scrittura e alla lettura del database.
Per avere una maggiore sicurezza ci conviene proteggere il database con una password da immettere direttamente in Access usando il menu contestuale.

:: I primi tentativi

Il nostro obbiettivo è fare in modo che i caratteri del testo da noi digitati siano irriconoscibili. Come possiamo farlo in modo semplice?
Cominciamo ad aggiungere 1 al codice ASCII di ogni singolo carattere. Quindi se scriviamo "SAURON" vedremo "TBYSPO". Un bel sistema, si, facile facile, anche troppo. Basta infatti scoprire che la lettera "A" in realtà è rappresentata con "B" che sarà semplice indovinare e ricavare tutte le informazioni. Ma noi abbiamo la potenza di un calcolatore ai nostri piedi, perché non farlo lavorare un po' di più? Proviamo a trasformare tutti i caratteri nel loro corrispondente ASCII. Ma siamo ancora troppo vulnerabili.

Ecco che "SAURON" Diventa "(83+1) + (65+1) + (85+1) + (82+1) + (79+1) + (78+1)



:: Cominciamo a fare sul serio

Dividiamo a questo punto il numero che rappresenta ogni singolo carattere in due differenti parti.
Per cui la S diverrebbe dapprima “83” e poi un 8 e un 3. A questo punto possiamo agire sulle due parti del carattere così ottenute in modo da rendere più difficile l’interpretazione. Adesso la nostra parola chiave è di fatto divisa in 12 variabili contenenti i frammenti delle lettere che compongono la parola stessa.
Ammettiamo di usare come parola chiave SAURON (83 + 65 + 85 + 82 + 79 +78) e che il testo in questo esempio sia “Non mi leggi”.
Dividendo la parola chiave in 12 variabili differenti, abbiamo di fatto diviso il codice ASCII in decimali e unità che metteremo poi in variabili fisse chiamate K1 e K2 per il primo carattere della parola chiave, K3 e K4 per il secondo e così via. Quindi in K1 e K2 ritroveremo rispettivamente i valori 8 e 3, in K3 e K4 6 e 5 eccetera.
A questo punto una volta inizializzate le variabili fisse andiamo a leggere la nostra stringa e creiamo altri gruppi di variabili, usando però una matrice dinamica perché non sapremo quanto è lungo il testo da criptare. Impostiamo una variabile **DIMMA** al numero massimo di caratteri in modo da sapere quante volte dobbiamo ricorrere alla cifratura dei caratteri.

:: Nel cuore della cifratura

Ora dobbiamo criptare in qualche modo la nostra frase contenuta nella stringa (Stringa).
Ci servono due variabili di controllo. **Giro**, una variabile numerica che ci fa capire a che punto della nostra parola chiave siamo e **Stringa_Codficata** che andremo a riempire di dati a mano a mano che li snoccioleremo.
Creando un semplice ciclo FOR <-> NEXT analizziamo Stringa carattere per carattere utilizzando come valore massimo DIMMA precedentemente inizializzato.
Con un’altra semplice istruzione interna al precedente ciclo, SELECT CASE Giro, faremo in modo di applicare a ogni carattere preso in esame una modifica che lo renderà criptato.

Ricordiamoci che

K1 = 8

K2 = 3

Il risultato è che come primi valori in Stringa_Codificata otterremo “N”= 78 = 7 + 8, che diventa (7 + K1) e (8+K2) e “o”=111 che diventa (11+K3) e (1+K4) eccetera. Quindi i valori che andremo a conservare in Stringa_Codificata saranno 15 e 11 per “N”, 17 e 6 per “o” e così via. A questo punto la prima lettera della stringa che abbiamo dato da criptare (“N”) è ora divisa in due differenti valori difficilmente riconducibili all’originale. Questa procedura verrà sviluppata su tutto il testo con un sistema che ogni volta va a riapplicare la parola chiave da capo. Per cui una lettera, ad esempio la “A”, non avrà lo stesso valore all’interno della stringa criptata perché tale valore viene dato dal prodotto di somme con numeri di riferimento sempre differenti in base alla posizione della stessa rispetto alla parola chiave. Per risalire al dato originale è necessario saperne il codice. Un programma automatico di decriptazione difficilmente potrà risalire al valore originale.
Riassumendo, in Stringa_Codificata i caratteri, che verranno scritti utilizzando [e] come separatori, sono: **”]15 11[”** poi seguiti da **“]17 06[”** eccetera.
Dobbiamo fare in modo che i due numeri siano sempre formati da due cifre, quindi nel caso del 6 aggiungiamo uno 0 davanti.
In più alla fine della nostra cifratura possiamo metterci anche una ciliegina. Basta applicare la funzione **Stringa_Codificata=StrReverse (Stringa_Codificata)**.

:: Procedura inversa

E adesso che abbiamo protetto la nostra frase come facciamo a leggere il testo? Seguiamo il procedimento inverso.
Prima di tutto prendiamo i dati dal database e, con la solita funzione **Stringa_Codificata=StrReverse (Stringa),** si invertono.
Dopo di che procediamo in modo inverso, ma con una differenza rispetto alla creazione della stringa. Infatti in questo caso sappiamo già cosa andiamo a pescare dal nostro pentolone. E sappiamo che i dati sono stati scritti a gruppi di sette caratteri. Quindi nel ciclo FOR<->NEXT useremo l’accorgimento di prendere a blocchi di 7 caratteri, come possiamo verificare da: **”]15 11[”**. Il gioco è fatto. Togliamo ai valori le rispettive parti della parola chiave. Per cui (15 - K1) = 7 e (11 - K2)=8 che messi insieme danno 78, che guarda caso equivale al codice ASCII della lettera “N”. Con poche righe di codice abbiamo generato il nostro sistema di cifratura personale.
Ah! A proposito, non lasciate sulla scrivania o sul PC la parola chiave leggibile da tutti! Mi raccomando!





Google Chrome

Dopo un mese dal lancio è tempo di esami

Che "beta release" significhi un programma non ancora definitivo ma abbastanza maturo per una prova sul campo è ormai chiaro per tutti, quindi usando un programma in tale fase di sviluppo tutti si aspettano qualche problema (grande o piccolo che sia, concettuale o semplicemente di prestazioni).

Nel caso di Chrome, il bilancio è stato tutto sommato positivo, se non altro per quanto riguarda le prestazioni promesse e l'aspetto estetico. Tuttavia alcuni nei, uno dei quali piuttosto grave, hanno spento parecchio l'entusiasmo del momento del lancio e lasciato un velo di perplessità tra gli utenti e gli operatori del settore. In queste pagine non vogliamo soffermarci troppo sulle caratteristiche del nuovo browser, cosa di cui abbiamo già parlato e che comunque è sotto gli occhi di tutti quelli che si prendono la briga di scaricarlo e provarlo; vogliamo invece mettere, come si suol dire, il dito nella piaga, facendo le pulci agli sviluppatori Google e spiegare per filo e per segno perché, a nostro avviso, Chrome non meritasse ancora di passare alla fase beta pubblica.

:: Asini, cavalli e muli

Ci è piaciuto molto l'esempio portato da Aviv Raff, un noto esperto di sicurezza informatica che pubblica in maniera chiara e comprensibile a tutti i risultati delle proprie ricerche sul suo sito (http://aviv.raffon.net), che ha scoperto per primo il problema. Se incrociamo un cavallo con un asino, otteniamo un mulo. Il mulo ovviamente in questo caso è proprio Chrome, che va a pescare dal patrimonio genetico di due illustri predecessori, Mozilla Firefox (dal quale ha mutuato alcuni concetti per quanto riguarda l'estetica e l'interfaccia utente) e Apple Safari (dal quale invece ha ereditato parte del core, nello specifico il sistema di rendering delle pagine). Niente lavoro originale, quindi, se non per mettere insieme frammenti di codice scritto da altri, adattandoli alla nuova collocazione. In più, Safari stesso può essere considerato quasi un "mulo", in quanto in parte si basa non su codice scritto ad hoc ma sulla popolare libreria di WebKit. Intendiamoci, questo non vuol dire che denigriamo il modo di lavorare del team di sviluppo di Google: è prassi normale ai giorni nostri basarsi sul lavoro già svolto da altri, soprattutto da quando il concetto di open source è diventato di dominio pubblico e ha raccolto i favori della maggior parte dei programmatori di tutto il mondo informatico.

:: Troppa fretta

Come abbiamo detto, Chrome basa la propria tecnologia di rendering delle pagine sul codice di Safari, in particolare sulla release 3.1 del browser di Apple. A sua volta, Safari 3.1 è scritto implementando la release 525.13 di WebKit. Fin qui come abbiamo detto niente di male, se non fosse che proprio questa release di WebKit era affetta da una grave falla di sicurezza: usando una debolezza del sistema era possibile per un sito Web maligno colpire con il cosiddetto Carpet Bombing (il download automatico di un file eseguibile, che ovviamente può essere maligno) il browser del visitatore.



Le versioni delle librerie usate: da notare WebKit 525.13.

Apple ha risolto il problema da sola, rilasciando la versione 3.1.2 di Safari che corregge questo e altri piccoli problemi, ma Google no, usando la release 3.1 delle librerie affetta dal problema. Perché mai? È questo che ci chiediamo, e l'unica risposta che ci viene in mente è la troppa fretta di lanciare la beta di Chrome, esponendo tutti gli utenti "occasionali" del browser a un grave rischio.

:: Ancora più fretta

Altro problema: basandosi su codice scritto per Mozilla Firefox, Chrome ha ereditato la capacità di scaricare ed eseguire controlli ActiveX, che non sempre sono benigni e utili per la navigazione (pare che siano stati riportati casi in cui questo comportamento è avvenuto in maniera trasparente per l'utente). A questo punto è chiaro dove sia il problema principale di Chrome: non tanto in questi bug, che concettualmente erano prevedibili e potevano essere risolti con ampio margine, ma proprio nella fretta con cui è stato reso disponibile al grande pubblico.

:: Carpet Bombing

Un sito dalle deprecabili intenzioni potrebbe inserire in una pagina codice che attivi automaticamente il download di un file .JAR con contenuti maligni. Nel caso di altri browser, il download viene posto in una apposita cartella o al limite sul desktop e viene chiaramente visualizzato mentre è in corso in una apposita finestra di dialogo. In Chrome, invece, viene creata una barra nella parte inferiore della pagina, in cui appare il nome del file in download sotto forma di pulsante. Basta un clic su questo pulsante da parte di un utente inesperto per trasferirne il controllo al sistema operativo che lo apre, lo salva o lo esegue secondo il caso. Avremo quindi il caso in cui si scarica un file .EXE, .COM o .BAT, in cui Explorer di Windows (nota: non Internet Explorer, stiamo parlando dell'interfaccia utente di Windows, che si chiama anch'essa Explorer), se opportunamente aggiornata con le ultime patch di sicurezza, mostra un avviso di sicurezza (e in questo caso anche un utente poco accorto non può non accorgersene e cadere vittima del tranello); diversamente nel caso invece di un file .JAR, cioè di un file che contiene un eseguibile Java, per il quale non viene emesso alcun avviso ma viene invece avviato JRE (Java Runtime Environment) ed eseguito a piè pari. Con tutte le conseguenze del caso.

:: La morale è sempre quella

Niente a che vedere con merendine al cioccolato (i più anzianotti tra voi sicuramente capiranno), due piccoli problemi presi da soli possono non essere preoccupanti, ma presi insieme possono diventare un vero guaio. Qui si unisce la leggerezza di Google, che ha basato il proprio codice su librerie preesistenti e di cui era ben nota la vulnerabilità, senza peraltro correggere il problema prima di lanciare il prodotto in test pubblico, alla leggerezza di Microsoft, che si ostina a riconoscere i file dalla loro estensione e non dal loro contenuto e che, per non si sa bene quale motivo, non ha inserito i file .JAR tra quelli che possono causare problemi se avviati con sufficienza.
In definitiva Chrome è bello, promette molto, però meglio non usarlo finché Google non si metterà a fare le cose un po' più seriamente. Nella speranza che il browser del famoso motore di ricerca non diventi un'altra di quelle iniziative in beta perenne. Staremo a vedere.

Privateer

FALSO ALLARME

Pochi giorni fa per qualche ora è stato impossibile scaricare il pacchetto di installazione di Chrome per chi usa l'antivirus Avast, che segnalava la presenza di un trojan (nella fattispecie Win32:Midgare-OI [trj]). Si trattava di un falso positivo, prontamente corretto con un tempestivo aggiornamento da parte del team di Avast. I sudori freddi però li abbiamo passati lo stesso...



HACKER ALLA REGIA

Con qualche trucco "domiamo" i motori grafici dei videogiochi per realizzare ottimi film. Ecco come si fa

La parola "hacking" può essere interpretato in tanti modi, ma il concetto di base è quello di modificare un oggetto, o una tecnologia, e fargli fare qualcosa per cui non è stato sviluppato in origine. Capita così che anche un "semplice" videogioco possa essere modificato per creare un film di qualità. Questa tecnica si chiama "machinima", termine che deriva da "machine cinema", e consiste nell'intervenire sulle tecnologie che danno vita al gioco preferito; per comandarlo in tutti i suoi aspetti e realizzare filmati degni di Hollywood. Modelli tridimensionali, livelli, animazioni, suoni, musiche... sono alcuni degli elementi pronti per essere riciclati nella nostra produzione cinematografica. E senza scendere a compromessi con la qualità, visto che



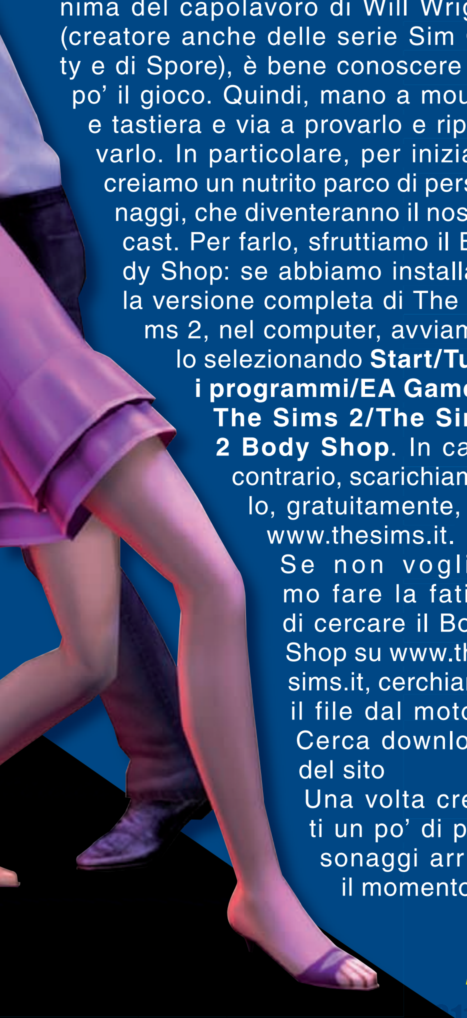
Se non vogliamo fare la fatica di cercare il Body Shop su www.thesims.it, cerchiamo il file dal motore Cerca download del sito.



la definizione grafica e sonora dei titoli videoludici più moderni non ha nulla da invidiare a quella delle TV e del cinema. Se, dunque, desideriamo diventare dei registi affermati ma non abbiamo a disposizione il becco d'un quattrino, vediamo com'è possibile sfruttare uno splendido e diffuso videogioco come The Sims 2, per fare del buon machinima. Ci sarà da divertirsi, garantito.

:: Giochiamolo, prima di tutto

Forte di oltre 100 milioni di copie vendute, nelle sue varie versioni, The Sims è di diritto il gioco PC più diffuso di tutti i tempi. Il secondo episodio, tra l'altro, vanta un motore grafico (cioè l'insieme delle funzioni che calcolano e visualizzano la grafica del gioco) di tutto rispetto e, soprattutto, ampiamente modificabile.
Per beneficiare delle funzioni machinima del capolavoro di Will Wright (creatore anche delle serie Sim City e di Spore), è bene conoscere un po' il gioco. Quindi, mano a mouse e tastiera e via a provarlo e riprovarlo. In particolare, per iniziare creiamo un nutrito parco di personaggi, che diventeranno il nostro cast. Per farlo, sfruttiamo il Body Shop: se abbiamo installato la versione completa di The Sims 2, nel computer, avviamolo selezionando **Start/Tutti i programmi/EA Games/The Sims 2/The Sims 2 Body Shop**. In caso contrario, scarichiamolo, gratuitamente, da www.thesims.it.
Se non vogliamo fare la fatica di cercare il Body Shop su www.thesims.it, cerchiamo il file dal motore Cerca download del sito
Una volta creati un po' di personaggi arriva il momento di passare al gioco vero e proprio: se lo dobbiamo ancora acquistare, procuriamoci insieme anche l'espansione Nightlife (si trova a prezzo scontato in parecchi negozi online). Non è obbligatoria per fare machinima con The Sims 2, ma estende non poco le possibilità cinematografiche del titolo.
Una volta creato il nostro cast, e aver preso un po' di dimestichezza col gioco, creiamo anche il nostro set virtuale. Avviamo il titolo selezionando **Start/Tutti i programmi/EA Games/The Sims 2/The Sims 2** e, dal menu principale, clicchiamo su Scegli un quartiere per giocare. Scorriamo la lista visualizzata e clicchiamo su Scegli un quartiere personalizzato. Poi, clicchiamo sullo scenario che preferiamo, specificando i parametri mancanti, come il nome e Scegli un terreno (Verde o Deserto). Una volta creato lo sfondo del set, piazziamoci un primo edificio. Possiamo "comprarlo", premendo il tasto F2 e selezionando quello desiderato, oppure costruirlo. Nel secondo caso, dopo aver premuto F2, selezioniamo Lotti vuoti e quindi la dimensione del lotto (Lotto medio va benone). A questo punto, diamo spazio alla fantasia, sfruttando gli strumenti messi a disposizione dall'interfaccia, per modificare il terreno del lotto e costruirci un ampio edificio. Come primo set, è più che sufficiente un edificio con quattro pareti, un pavimento, una porta e qualche finestra.



Scene notturne o "danzerecce"? L'espansione Nightlife è altamente consigliata!

:: Finalmente l'hacking

Una volta che abbiamo cast e set, siamo pronti a modificare The Sims 2 per trasformarlo in un potente strumento per la creazione di machinima.
Usciamo dal gioco e, da Windows, andiamo nella sotto-cartella **Programmi/EA Games/The Sims 2/TSData/Res/Config**. Da qui, apriamo col Blocco note, o un editor di testo, il file **globalProps.xml**.
Se utilizziamo Windows Vista, a causa delle impostazioni di sicurezza, potrebbe essere necessario copiare il file altrove, per modificarlo, e quindi ricopiarlo nella sotto-cartella, sostituendolo all'originale (in questo caso, creiamo una copia di riserva). Una volta aperto, cerchiamo la stringa:

```
<AnyBoolean
key="allowCustomContent"
type="0xcba908e1">true</
AnyBoolean>
```

Sotto a questa, aggiungiamo la stringa

```
<AnyBoolean key="testingCheatsEn
abled" type="0xcba908e1">true</
AnyBoolean>
```

E salviamo il file. di fatto, abbiamo appena attivato la modalità "cheat" di The Sims 2. Avviamo il gioco, carichiamo il quartiere (il nostro "set") creato poco fa e, dalla schermata di gioco, premiamo la combinazione di tasti Ctrl+Shift+C. Nella parte superiore dello schermo compare una riga. Scriviamo qui l'istruzione: e premiamo Invio.

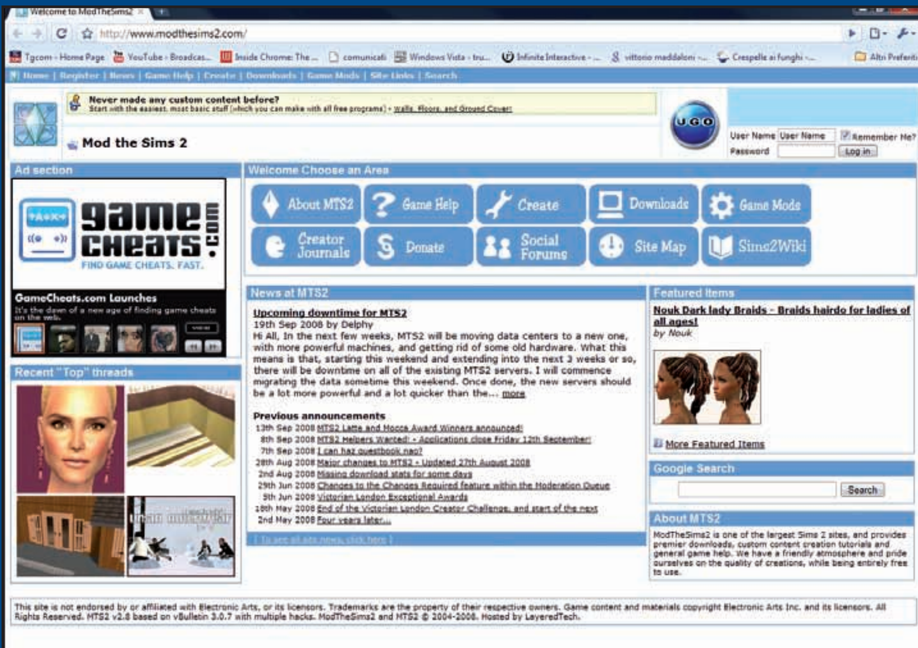
```
boolProp enablePostProcessing true
```

Premiamo di nuovo la combinazione Ctrl+Shift+C, scriviamo il comando, e premiamo Invio.

```
boolProp testingCheatsEnabled true
```

Seguiamo la medesima procedura per inserire altri comandi:

```
boolProp useEffects false
AllMenus On
moveObjects On
Aging Off
```



Il principale sito dedicato al modding e hacking del capolavoro di Will Wright è www.modthesims2.com.

Una volta attivati questi "cheat", usciamo dal gioco e andiamo a registrarci, gratuitamente, nel sito www.modthesims2.com.
Quindi, scarichiamo il file **TS2Studios0_4.BETA.zip**, che troviamo al link **http://modthesims2.com/showthread.php?t=100738**. Si tratta di The Sims 2 Studio, che aggiunge le funzionalità da studio cinematografico al gioco. Apriamo il file scaricato ed estraiamo il file **TS2Studios04B.package**, che troviamo al suo interno, nella **cartella documenti/EA Games/The Sims2/downloads**. Avviamo The Sims 2 e prepariamoci a girare il nostro primo film machinima. Innazitutto, creiamo una "famiglia", utilizzando i personaggi del cast e associando loro le caratteristiche desiderate, come le Aspirazioni. Fatto questo, carichiamo il nostro "quartiere" e sistemiamo all'interno del set i vari componenti della "famiglia".
Seguendo una procedura simile, aggiungiamo al quartiere un secondo edificio e, al suo interno, altri attori virtuali: lo useremo come "serbatoio" di attori pronti da inserire nel set.
Alla fine, ci ritroviamo con un quartiere con due edifici, uno dei quali è il set vero e proprio, con all'interno di ciascuno degli attori. Adesso aggiungiamo un po' di denaro al conto virtuale di ciascun edificio: ci basta entrare al suo interno, premere la combinazione Ctrl+Shift+C, digitare **motherlode** e premere Invio
Poi, andiamo all'interno dell'edificio-set, premiamo F5, selezioniamo **Video/Livello prestazioni** e assicuriamoci che **Nascondi gli oggetti** sia impostato su Off. Torniamo nella schermata di gioco e, da qui, premiamo Ctrl+Shift+C. Digitiamo **letterbox 0.2** e premiamo Invio. Poi, scriviamo exit e premiamo ancora Invio, per chiudere la finestra d'inserimento dei comandi.

:: Qualche movimento di camera

È il momento di disattivare l'audio: così la registrazione video sarà più fluida e potremo inserire un doppiaggio "serio" una volta realizzato il film.
Dalla schermata di gioco, premiamo F5 e clicchiamo su **Opzioni della visuale**. In **Acquisizione audio** dei filmati spuntiamo la casella Off e, già che ci siamo, impostiamo **Tempo max registrazione filmati** a un valore superiore ai 60 secondi predefiniti, per esempio 600. Premiamo F1 e torniamo al gioco.
Una volta nel set, premiamo il tasto P, per mettere in pausa la partita, e posizioniamo attori e oggetti vari e assortiti. Fatto questo, premiamo V per avviare le "riprese". Spostiamo la telecamera di gioco (W, A, S o D): un "movimento di telecamera" su una scena fissa, come primo esperimento, non è niente male. Alla fine, premiamo V di nuovo e salviamo il filmato realizzato.
Per dare movimento al tutto, togliamo la pausa e filmiamo i nostri attori mentre si animano. Dato che, dopotutto, sono gestiti anche dall'intelligenza artificiale, qualche scena rischia di diventare fin troppo "sponta-



Un modo semplice e veloce per fare soldi. Ma funziona solo in The Sims 2...



Ecco attivato il formato "letterbox", che si sposa a meraviglia con i nuovi televisori panoramici in 16:9.



Prima di iniziare con le riprese, è sempre meglio fare casting per selezionare gli attori e le comparse.

nea" e slegata dalle nostre direttive: in fondo vivono di vita propria, no? In questo caso niente paura: dal filmato ottenuto taglieremo le scene inadatte o superflue, con un software di montaggio video.

:: Tutti ai nostri comandi

C'è un altro modo per controllare senza esitazioni i Sim-attori. Poco fa abbiamo creato due edifici con due distinti cast che li abitano.

Ora, aggiungiamo un terzo edificio, costruendolo privo di porte e finestre: lo chiamiamo, per questo, "set-prigione". Tenendo premuto il tasto Shift, clicchiamo quindi sulla rispettiva cassetta della posta, e selezioniamo **Invite all Neighbours**.

Una volta che gli attori arrivano davanti al set-prigione, premiamo il tasto F2 (Modalità compra), premiamo la combinazione Ctrl+Shift+C e attiviamo il cheat **MoveObjects true**.

Attivato questo, clicchiamo su un attore e "trasciniamolo" all'interno del set-prigione. Poi, tenendo premuto Shift, clicchiamo di nuovo sull'attore appena spostato e, nel menu visualizzato, selezioniamo **MAKE SELECTABLE**. Da questo momento, l'attore passa sotto il nostro totale controllo.

Per ampliare le azioni a disposizione dei nostri attori, sfruttiamo anche il **The Sims 2 Studio** installato precedentemente. Dalla schermata di gioco, e con un attore selezionato, premiamo F2 (Modalità compra); e clicchiamo poi su **Hobby**. Scorrendo la lista di oggetti, vediamo una "scatola nera".

Facciamoci sopra un doppio clic e posizionamola poi in un punto del set, meglio se nascosto dalle riprese. Passiamo alla **Modalità vivi** e clicchiamo sulla scatola. Viene così visualizzato un completo menu, ricchissimo di animazioni alternative pronte per rendere ancora più cinematografico il nostro film machinima. Sperimentiamole pure in tutta la loro spettacolarità: dal pianto disperato alla risata spensierata, c'è davvero tutto per accontentare anche i registi più esigenti.

E poi, quando si tratta di effettuare nuove riprese, seguiamo pure la procedura vista: un "ciak", anche virtuale, che potrebbe presto spianarci le porte di Hollywood!

Riccardo Meggiato



The Sims 2 Studio aggiunge tante, entusiasmanti, animazioni per il machinima.



Bluetooth navigation

Usiamo la ADSL di casa per navigare con il telefonino Bluetooth

Grazie al collegamento via bluetooth il telefonino di fatto diventa un terminale della tua LAN che puoi usare, ad esempio, per fare chiamate VoIP senza dover pagare alcun costo aggiuntivo che nei limiti dei 30 metri massimi previsti dalla trasmissione bluetooth equivale a un vero e proprio cordless. Possiamo usarlo per rispondere a MSN, per controllare la posta, per accedere a IRC e tutto col nostro amato telefonino. E se il telefonino ha symbian o windows mobile si possono fare molte delle cose che faremmo con un pc!
Chiaramente per permettere al telefonino di navigare anche il pc dovrà disporre di questo collegamento, ma è sufficiente acquistare una chiavetta USB Bluetooth da 20€ c.a.

:: Cosa dobbiamo fare

Prima di tutto si deve scaricare l'ultima versione disponibile di Hiisi, la v1.6.3 (http://hiisi-proxy.blogspot.com/2007/06/download-hiisi-proxy.html).
Una volta decompresso l'archivio ci troveremo tre cartelle, di cui ci interessano le prime due:

1.\Hiisi
2.\Pihatonttu

Ora dovremo configurare il software sul telefonino e sul pc connesso a Internet.

:: Configurazione del telefonino

Dentro la prima cartella c'è il sprogramma che dovremo installare a bordo del telefonino con il software per il trasferimento dati in dotazione (es. per Nokia si userà PC Suite). Una volta installato troveremo una nuova icona nel menu chiamata "Hiisi Proxy". Ora dobbiamo creare un nuovo profilo per gestire il collegamento via bluetooth.
Su Nokia, selezioniamo Tools → settings → connection → access points → options → create new access point. Si può scegliere il nome che si preferisce, ad esempio "BT", lasciando i parametri di base ai valori di default a meno che



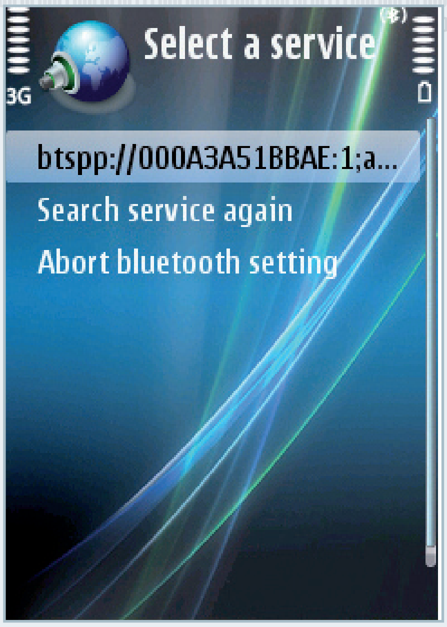


non ci sia qualche limitazione imposta dal provider (vedi più avanti).
Selezioniamo Options → Advanced settings e in fondo impostiamo 127.0.0.1 come indirizzo proxy server, 1234 come porta del proxy e salviamo il profilo. Questi valori sono quelli di default che andrà a usare il nostro proxy sul pc.
Ora apriamo Hiisi, dopo aver abilitato Il bluetooth sia sul PC che sul telefonino e cerchiamo il PC da Hiisi.



Una volta selezionato il pc, dovremo cercare la seriale virtuale abilitata sul PC (vedremo un indirizzo del tipo





btspp://...). Lo selezioniamo ed avviene la connessione via bluetooth tra il proxy client e il proxy server. Può succedere che la connessione dopo un po' vada in idle e si disconnetta. È sufficiente ripetere la connessione andando su Settings e spuntanto Check now prima di dare OK.

:: Configurazione del PC

Apriamo con Blocco note (o il proprio editor di testo preferito) il file \Pihatonttu\Pihatonttu_localhost.cmd e va modificata la porta COM7 con la COMxx che vogliamo associare al collegamento bluetooth sul PC e salvato il file. Per identificare la porta dedicata al collegamento bluetooth seriale basta andare su Pannello di controllo → Bluetooth e verificare qual è la seriale che è stata assegnata e risulta attualmente impegnata.
Su PC con Windows, se non ce l'abbiamo già, andremo a installare l'ultima versione di Java Runtime Environment (JRE) scaricandola direttamente dal sito della Sun (http://java.sun.com/javase/downloads/index.jsp). Per verificare che sia installata basta digitare da linea di comando (Start → Esegui → cmd + Enter) **"java -version"**.
Ora clicchiamo due volte sopra **"Pihatonttu_localhost.cmd"** per lanciarlo: in questo modo avremo lanciato il servizio di proxy sul nostro pc che resta in attesa delle richieste che verranno dal telefonino.

Questo servizio si occuperà di accettare le richieste provenienti dal telefonino e instradarle verso il router ADSL e mostrerà tali richieste man mano perverranno nella finestra di log.

:: Alcuni problemi segnalati

Purtroppo a seconda dell'hardware di gestione del bluetooth potrebbero verificarsi alcuni problemi di comunicazione tra il pc e il telefonino o difficoltà nel determinare quale sia la porta COM da utilizzare.

In particolare, è utile verificare che il pairing tra le due periferiche bluetooth sia funzionante (ad esempio che si possa fare il trasferimento dei dati di rubrica) e determinare con certezza qual è la porta utilizzata per la trasmissione dal telefonino verso un servizio attivo su una com virtuale del pc:

- nel caso si utilizzi un driver BlueSoleil, impostare dal menu My Service → Property → Port number corrispondente a **"Serial Port A, B"**;
- nel caso si utilizzi un driver Toshiba, dal Pannello di controllo → Bluetooth Local COM, identificare la COM dove compare **"Local-COM Server"**;
- nel caso si utilizzi il driver generico di Windows XP, dal Pannello di controllo → Bluetooth Device, aggiungere una porta COM definita come **"Incoming"**;
- nel caso si utilizzi il driver WIDCOMM, dal Pannello di controllo → Bluetooth Configuration → Local Services, aggiungere un servizio bluetooth-seriale.

Nel nostro test, con una Sim della TRE abbiamo avuto diversi problemi per connettere un Nokia 6680, finché non abbiamo capito che la Sim forza comunque una verifica sull'esistenza di copertura GPRS/UMTS prima di autorizzare il telefonino a navigare. Per risolvere questo problema è stato sufficiente aggiungere nel profilo "BT" alla voce Access point name **"tre.it"** che compare nel profilo di default del provider. A seconda dei casi può essere inoltre utile lanciare **Pihatonttu.cmd** invece di **Pihatonttu_localhost.cmd**.

Massimiliano Brasile

Finalmente in edicola la prima rivista

PER SCARICARE ULTRAVELOCE

TUTTO quello che vuoi

NUOVA!



Sprea editori ITALY

Chiedila subito al tuo edicolante!